Microsoft

Microsoft Security Intelligence Report

Volume 19 | January through June, 2015

Featured Intelligence

Authors

Charlie Anthe
Cloud and Enterprise Security

Patti Chrzan
Microsoft Digital Crimes Unit

Elia Florio
Microsoft Malware Protection Center

Chad Foster
Bing

Paul Henry
Wadeware LLC

Jeff Jones
Corporate Communications

Nam Ng
Worldwide Cybersecurity & Data Protection

Niall O'Sullivan
Microsoft Digital Crimes Unit

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Anthony Penta
Safety Platform

Ina Ragragio
Microsoft Malware Protection Center

Tim Rains
Worldwide Cybersecurity & Data Protection

Paul Rebriy
Bing

Contributors

Peter Cap
Microsoft Malware Protection Center

Bulent Egilmez
Office 365 - Information Protection

Tanmay Ganacharya
Microsoft Malware Protection Center

Kathryn Gillespie
Microsoft IT

Jeff Glover
Microsoft IT

Roger Grimes
Microsoft IT

Satomi Hayakawa
CSS Japan Security Response Team

Ben Hope
Microsoft Malware Protection Center

Yurika Kakiuchi
CSS Japan Security Response Team

Jenn LeMond
Microsoft IT

Alisha Mark
Corporate Communications

Dolcita Montemayor
Microsoft Malware Protection Center

Daric Morton
Microsoft Services

Jeong Mun
Microsoft Malware Protection Center

Cody Nicewanner
Operating Systems Group

Wendi Okun
Legal & Corporate Affairs

Ferdinand Plazo
Microsoft Malware Protection Center

Laura A. Robinson
Microsoft IT

Norie Tamura
CSS Japan Security Response Team

Steve Wacker
Wadeware LLC

Vladimir Zubko
Microsoft Malware Protection Center

Table of contents

About this report

The *Microsoft Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, malware, and unwanted software. Past reports and related resources are available for download at www.microsoft.com/sir. We hope that readers find the data, insights, and guidance provided in this report useful in helping them protect their organizations, software, and users.

Reporting period

This volume of the *Microsoft Security Intelligence Report* focuses on the first and second quarters of 2015, with trend data for the last several quarters presented on a quarterly basis. Because vulnerability disclosures can be highly inconsistent from quarter to quarter and often occur disproportionately at certain times of the year, statistics about vulnerability disclosures are presented on a half-yearly basis.

Throughout the report, half-yearly and quarterly time periods are referenced using the *n*H*yy* or *n*Q*yy* formats, in which *yy* indicates the calendar year and *n* indicates the half or quarter. For example, 1H15 represents the first half of 2015 (January 1 through June 30), and 4Q14 represents the fourth quarter of 2014 (October 1 through December 31). To avoid confusion, please note the reporting period or periods being referenced when considering the statistics in this report.

Conventions

This report uses the Microsoft Malware Protection Center (MMPC) naming standard for families and variants of malware. For information about this standard, see "Appendix A: Threat naming conventions" on page 105 of the full report. In this report, any threat or group of threats that share a common unique base name is considered a family for the sake of presentation. This consideration includes threats that may not otherwise be considered families according to common industry practices, such as generic detections. For the purposes of this report, a threat is defined as a malware or unwanted software family or variant that is detected by the Microsoft Malware Protection Engine.

Foreword

Welcome to Volume 19 of the *Microsoft Security Intelligence Report (SIR)*. I've contributed to the SIR for almost ten years now. If I had to describe how the threat landscape has changed during that time using only one word, I'd say it's "cumulative."

Ten years ago we reported on a range of threats that included trojans, worms, trojan downloaders & droppers, exploits, bots (backdoor trojans), among others. These types of threats were primarily motivated by a desire to disrupt networks, as worms did years earlier, or to seek profit.

Fast forward ten years and we still see the same categories of threats and even some of the same threat families employed. During this time, attackers have had to evolve their tactics to get malware onto computers that have also been evolving with continuously elevating security levels. As vulnerabilities in operating systems have become harder to find and exploit, attackers have relied increasingly on social engineering to compromise computer systems.

In addition to these types of attacks, we have seen more threat actors with different motivations emerge over the years, including hacktivists and practitioners of military and economic espionage. Rogue security software or fake antivirus software that was used to trick people into installing malware and disclosing credit card information to attackers has been replaced by ransomware that seeks to extort victims by encrypting their data. Commercial exploit kits now dominate the list of top exploits we see trying to compromise unpatched computers, which means the exploits that computers are exposed to on the Internet are professionally managed and constantly optimized at an increasingly quick rate. Targeted attacks have become common as opposed to the exception.

Attackers continue to try to use the tactics that they did years ago, and have added to their repertoire of dirty tricks. This is why I use the word "cumulative" to describe how things have changed. If I could use a second word to describe how they have changed I would use "accelerated." The focus and pace that some attackers have been demonstrating recently have certainly increased over time.

Notice I didn't use the word "advanced." Although attackers have accumulated more tricks and tactics and seem to be using them in a more focused, fast-paced way, they still focus on a relatively small number of ways to compromise computers, including:

- Unpatched vulnerabilities
- Misconfigured computers
- Weak passwords
- Social engineering

The great news if you are a CISO or security professional is that you've never had so much information and so many security capabilities and tools as you do today to defend your organization's data.

Please enjoy the report.

Tim Rains
Chief Security Advisor
Enterprise Cybersecurity Group
Microsoft

Featured intelligence

STRONTIUM: A profile of a persistent and motivated adversary

A research team at the Microsoft Malware Protection Center (MMPC) proactively monitors the threat landscape for emerging threats. Part of this job involves keeping tabs on targeted attack groups, which are often the first ones to introduce new exploits and techniques that are later used widely by other attackers. One such group, which Microsoft has code-named STRONTIUM, is of particular interest because of its aggressive, persistent tactics and techniques, and its repeated use of new zero-day exploits to attack its targets. Microsoft is sharing some of the information it has gathered on this prominent attack group in the hope that it will raise awareness of the group's activities and help organizations take immediate advantage of available mitigations that can significantly reduce the risks that they face from this and similar groups.

Adversary profile

STRONTIUM has been active since at least 2007. Whereas most modern untargeted malware is ultimately profit-oriented, STRONTIUM mainly seeks sensitive information. Its primary institutional targets have included government bodies, diplomatic institutions, and military forces and installations in NATO member states and certain Eastern European countries. Additional targets have included journalists, political advisors, and organizations associated with political activism in central Asia. *STRONTIUM* is Microsoft's code name for this group, following its internal practice of assigning chemical element names to activity groups; other researchers have used code names such as *APT28*,[1] *Sednit*,[2] *Sofacy*,[3] and *Fancy Bear* as labels for a group or groups that have displayed

---

[1] *APT28: A Window into Russia's Cyber Espionage Operations?*, FireEye, Inc., October 14, 2014, https://www2.fireeye.com/apt28.html.

[2] Loucif Kharouni et al., *Operation Pawn Storm: Using Decoys to Evade Detection*, Trend Micro, October 22, 2014, www.trendmicro.com/vinfo/us/security/news/cyber-attacks/pawn-storm-espionage-attacks-use-decoys-deliver-sednit.

[3] *Tactical Intelligence Bulletin: Sofacy Phishing*, PwC, October 22, 2014, pwc.blogs.com/files/tactical-intelligence-bulletin---sofacy-phishing-.pdf.

activity similar to the activity observed from STRONTIUM. The group's persistent use of spear phishing tactics and access to previously undiscovered zero-day exploits have made it a highly resilient threat.

How STRONTIUM attacks a target

STRONTIUM primarily uses two kinds of attack. It uses *spear phishing*—phishing attempts targeted at specific individuals—to perform reconnaissance and steal login credentials to gather information about potential high-value targets associated with the institution under attack. Following the reconnaissance phase, it uses a variety of methods to infect the computers of high-value targets with malware, often by exploiting previously unknown vulnerabilities in browser add-ons and other software.

Whereas most modern untargeted malware is ultimately profit-oriented, STRONTIUM mainly seeks sensitive information.

Reconnaissance and target identification

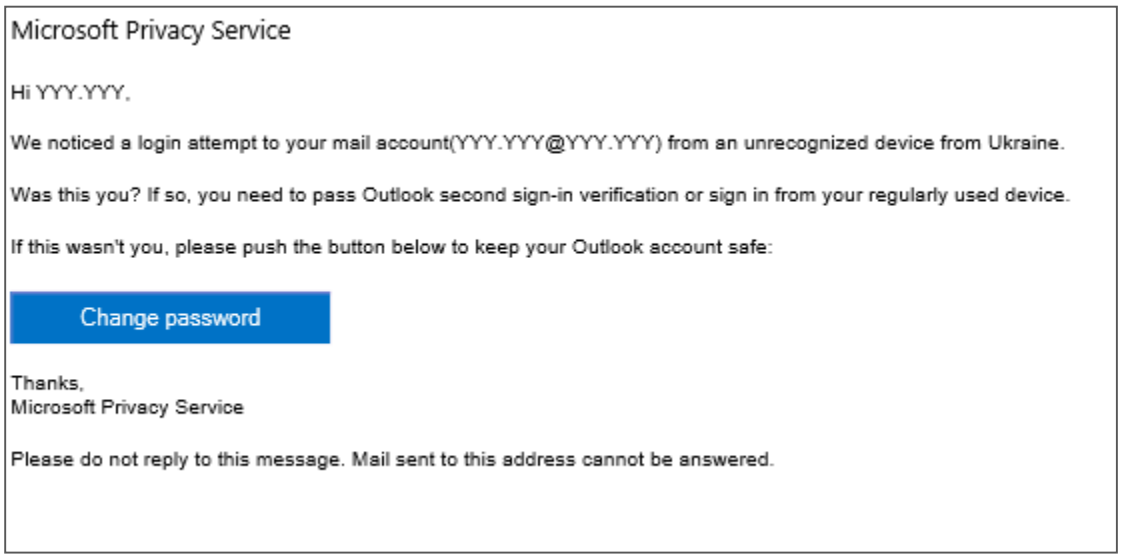
STRONTIUM typically begins its attack on an institution by identifying and profiling potential victims with connections to the institution. Microsoft has seen indications that STRONTIUM relies on open-source intelligence (OSINT), such as email lists and information harvested from public forums or social networking sites, to identify targets for spear phishing. Microsoft also believes that STRONTIUM relies on past successful phishing attacks to augment its dataset, by making use of any email communications it can identify between prior targets and the current target.

STRONTIUM casts a wide net with its reconnaissance activities, seeking login credentials for email and other systems from a large number of people, which it then weeds through to assess its value. Microsoft believes STRONTIUM used its spear phishing attacks to target several thousand individuals during the first half of 2015. Although STRONTIUM isn't choosy with its targets, it is persistent. When STRONTIUM identifies an individual to target, the group will repeatedly conduct spear phishing attacks against it over a long duration, possibly a year or more, until one of the attempts succeeds.

STRONTIUM's spear phishing modus operandi focuses on making the recipient concerned about unauthorized use of an account. A recent attack campaign involved sending messages with the subject line "Privacy alert" purporting to originate from a well-known email service, informing the user that their account

has been accessed from an unrecognized device in a different country. Because the targeted individuals are often professionals who have access to sensitive information, this can be an effective way to entice users to click a "change password" link that actually leads to a webpage under the attacker's control.

Figure 1. An example of a credential-stealing spear phishing message sent by STRONTIUM



Typically, the link will lead to a domain name that is similar to a legitimate domain name used by the service in an effort to fool the user into thinking the message is legitimate. Figure 2 lists some examples.

Figure 2. Examples of domain names spoofed by STRONTIUM in recent attacks

Legitimate domain name	Spoofed domain name controlled by STRONTIUM
accounts.google.com	accounts.g00qle.com
us-mg6.mail.yahoo.com	us-mg6mailyahoo.com
profile.live.com	privacy-live.com
mail.ukr.net	mail-ukr.net
www.nato.int	nato-news.com
www.bbc.com	bbc-press.org
www.osce.org	osce-press.com
www.eff.org	electronicfrontierfoundation.org

If the attack is successful, STRONTIUM uses the captured credentials to access the victim's email account to identify additional targets and for additional analysis and attacks. Even if the recipient doesn't enter their login credentials

into the malicious webpage, the act of clicking the link can provide STRONTIUM with valuable information. In addition to providing STRONTIUM with the recipient's IP address, clicking the link transmits a user-agent string to the web server that typically includes details about the recipient's browser and operating system versions, and sometimes includes information about the browser add-ons the recipient is using. This can provide STRONTIUM with insight into what software is deployed in the organization, and possibly help it plan future drive-by download activities.

Figure 3. JavaScript is used to collect information about the visitor's browser for drive-by download attacks

```
    string_of_json += "\"plugins\":[ ";
    //string_of_json += DetectJavaForMSIE();
    if(navigator.userAgent.indexOf("MSIE") > -1 || navigator.userAgent.indexOf(

        string_of_json += DetectJavaForMSIE();
        string_of_json += DetectFlashForMSIE();
        string_of_json += EnumeratePlugins();
        //string_of_json += DetectPdfForMSIE();
        //string_of_json += DetectFlashForMSIE();

    }
    else {
        string_of_json += EnumeratePlugins();
    }
    string_of_json = string_of_json.substring(0, string_of_json.length - 1);
    string_of_json += "]";
    var st = string_of_json_start + string_of_json + string_of_json_end;
    return st;
}

function getXmlHttpRequest() {
```

```
function xmlHTTPResponseHandler()
{
    var url = "http://www.nato.int/cps/en/[redacted].htm";
    if( xmlHttp.readyState == 4 && xmlHttp.status == 200 ) {
        url = xmlHttp.responseText;
        window.location.replace(url);
    }
```

Attacking the target

The ultimate goal of the reconnaissance phase is to compile a list of high-value individuals who have information or access that STRONTIUM wants. With this list at hand, the group moves to the next phase of operations: installing malware on

the high-value targets' computers, and thereby gaining access to the institution's network.

STRONTIUM primarily uses email to deliver malware to targeted individuals, although some researchers have reported delivery through social networking channels as well. Typical messages, such as the one shown in Figure 4, are tied to current events: an upcoming conference, for example, or a real world news event in which the recipient might be interested. STRONTIUM's email senders are usually associated with well-known email providers, and use plausible-seeming names and titles that are designed to give the messages credibility. Depending on the specific attack used, the message typically includes a link for "additional information," which will launch a drive-by download or social engineering attack when clicked. Other messages include malicious attachments instead of links, typically a document file containing an exploit.

Figure 4. An example of a lure email message sent by STRONTIUM

```
Subject: Mission_In_Central_African_Republic

*Dear Sir!*

Please be advised that The Spanish Army personnel and a large number of the
Spanish Guardia Civil officers
currently deployed in the Central African Republic (CAR) as part of the
European EUFOR RCA mission will return
to Spain in early March as the mission draws to a close.

Visit
http://eurasiaglobalnews.com/YYY-spains-armed-forces-conclude-mission-central-
african-republic/
for the addition info.

*Best regards,*

*Capt. John Smith, Defence Adviser, Public Diplomacy Division NATO,
Brussels defence.adviser.smith@gmail.com <defence.adviser.smith@gmail.com>*
```

Little is known about how and what information STRONTIUM gathers to tailor its attacks to specific high-value individuals. As discussed earlier, the user-agent and potential fingerprinting information gathered from phishing victims may play a part in planning the individual attacks by giving the group insight into what software may be in widespread use within the institution. In general,

STRONTIUM can take advantage of a variety of attacks that span general tactics and cover a wide range of technologies, including zero-day exploits.

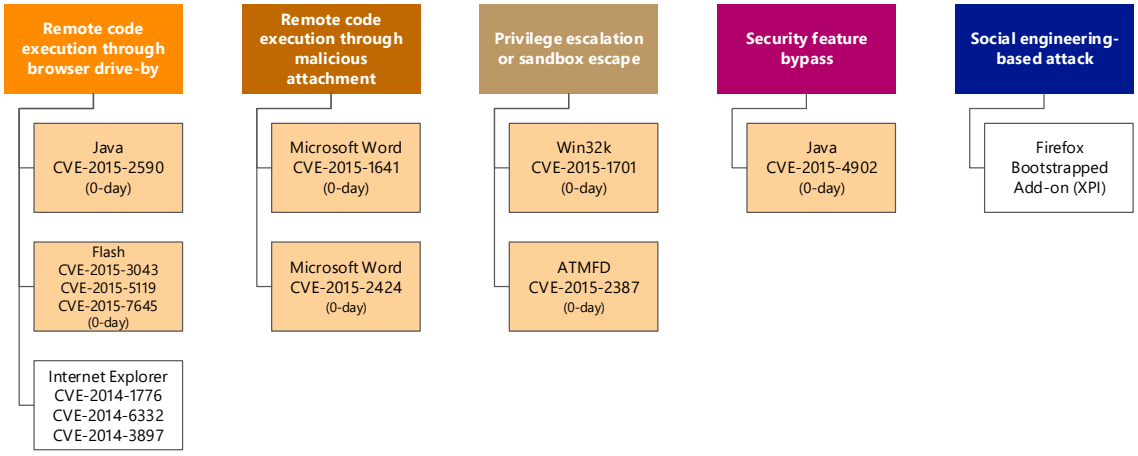
Zero-day exploits—exploits that target vulnerabilities for which the affected software vendor has not yet released a security update—form a significant part of STRONTIUM's arsenal. It is not yet clear whether the group researches vulnerabilities and develops the exploits themselves, or purchases them on the black market.

Microsoft researchers have observed STRONTIUM moving swiftly to take advantage of newly disclosed vulnerabilities; notably, the group deployed a number of zero-day exploits disclosed in a July 2015 leak of information from the security company Hacking Team. In other cases, STRONTIUM deployed exploits within days of a vendor releasing a security update that addressed the associated vulnerability, relying on the fact that not everyone installs security updates immediately after they are published.

Zero-day exploits form a significant part of STRONTIUM's arsenal.

The exploits used by STRONTIUM include a wide range of products from multiple vendors, including Adobe Flash Player, the Oracle Java Runtime Environment (JRE), Microsoft Word and Internet Explorer, and some components of the Windows kernel. Figure 5 lists some of the exploits used by STRONTIUM in recent campaigns, including a number of zero-day exploits (shaded). All of the vulnerabilities listed in Figure 5 were quickly addressed by security updates as part of the vendors' rapid response processes. (See "Guidance" on page 16 for information about how organizations can use up-to-date software to defend against targeted attacks.)

Figure 5. Some of the exploits used by STRONTIUM in attack campaigns in 2014 and 2015



In addition to using zero-day exploits, STRONTIUM also makes use of exploits that target older vulnerabilities for which security updates have been available for a long time. Microsoft believes that in some cases, the group learns during the reconnaissance phase that the targeted institution may be exposed to risks by running older or out-of-support platforms and software, by not testing and applying security updates quickly, or by not taking advantage of the latest mitigations and defense mechanisms shipped with more recent product versions—and then acts accordingly.

In a development observed in October 2015, the shellcode that executes after a successful memory corruption exploit displayed a number of characteristics that researchers had not observed from the malware previously:

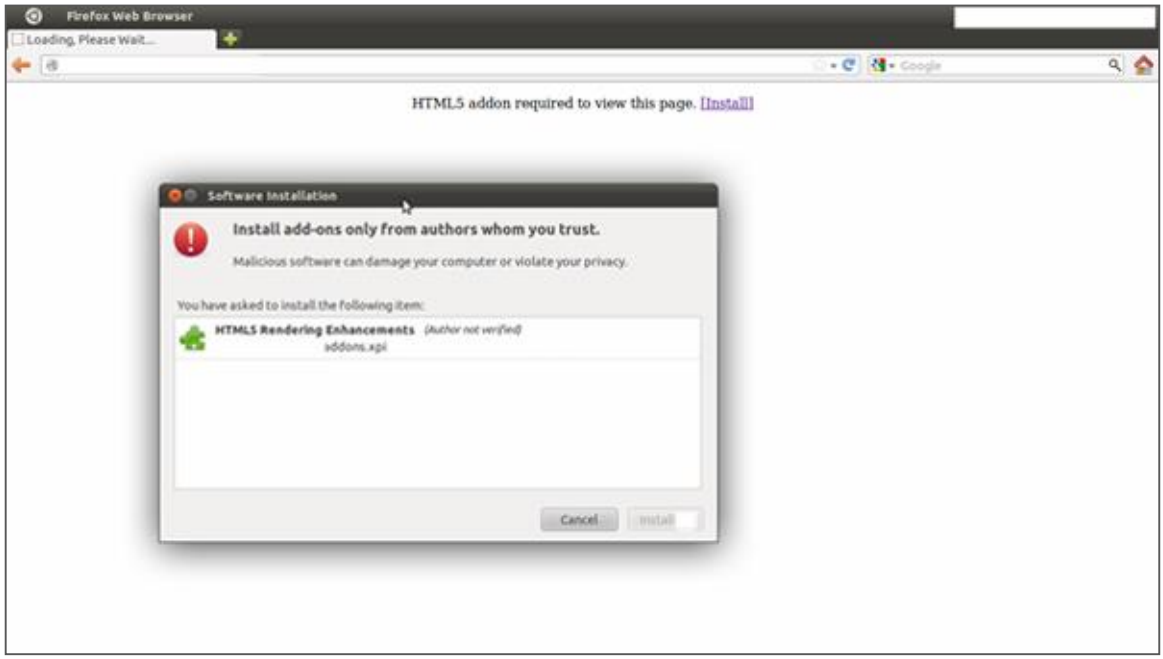
- API resolution: ROR 0x0D hashing, resolution made just before using the API
- Downloader: usage of HttpQueryInfo and WININET to fetch remote payloads in memory
- Compression: usage of ntdll!RtlDecompressBuffer()LZNT1 compression for remote payloads
- Privilege escalation: executed as DLL, but in-memory (diskless)

Figure 6. In-memory decompression and execution of remote payloads performed by STRONTIUM shellcode

```
1000025B
1000025B                            decompress:
1000025B 89 85 20 09 00 00                      mov     [ebp+shStru.ptrBuf4_rwx300000], eax
10000261 8D BD 24 09 00 00                      lea     edi, [ebp+shStru.FinalUncompressedSize]
10000267 57                                     push    edi
10000268 8B BD 08 09 00 00                      mov     edi, [ebp+shStru.CompressedBufferSize]
1000026E 57                                     push    edi
1000026F 8B BD 0C 09 00 00                      mov     edi, [ebp+shStru.ptrBuf2_rwx_download] ;
10000275 57                                     push    edi
10000276 68 00 00 30 00                         push    300000h         ; UncompressedBufferSize
1000027B 50                                     push    eax             ; UncompressedBuffer
1000027C 68 02 00 00 00                         push    COMPRESSION_FORMAT_LZNT1
10000281 68 84 01 E2 77                         push    77E20184h
10000286 FF D5                                  call    ebp             ; ntdll32!RtlDecompressB
10000288 8B 85 28 09 00 00                      mov     eax, [ebp+shStru.hWininet] ; passing WIN
1000028E 50                                     push    eax
1000028F 8B 85 20 09 00 00                      mov     eax, [ebp+shStru.ptrBuf4_rwx300000]
10000295 FF D0                                  call    eax             ; call 1st payload
10000297 E9 60 04 00 00                         jmp     loc_100006FC
```

In addition to relying on exploits, STRONTIUM also uses social engineering to trick victims into installing malware. Since March of 2015, for example, Microsoft has observed STRONTIUM successfully compromising Mozilla Firefox users by convincing them to install a malicious browser add-on based on a publicly available module ("Bootstrapped Addon Social Engineering Code Execution") developed for the Metasploit security testing framework.

Figure 7. STRONTIUM installs malware via a malicious bootstrapped add-on in Mozilla Firefox



Establishing control

After gaining administrative privileges on the computer through an exploit or social engineering, STRONTIUM uses a dropper to deploy a backdoor component, CORESHELL, which eventually downloads other modules. (Microsoft products sometimes detect the primary components as variants in the Win32/Foosace family, although the group has used other malware in the past.) The DLL backdoor is installed via execution of rundll32 with an export named "*init*" or "*InitW*." The dropper deletes itself after execution, while the DLL backdoor and any additional components are typically copied under the following folders:

- C:\Program Files\Common Files\Microsoft Shared\MSInfo\
- C:\Users\<*user name*>\AppData\Local\Microsoft Help\
- C:\ProgramData\

The dropper also writes the command and control (C&C) configuration information to the registry or an encrypted file. This strategy complicates forensic discovery of the attacker's infrastructure if the backdoor DLL is discovered, because the configuration information must be located separately.

Figure 8. Command & control configuration locations used by STRONTIUM

Format	Path
Registry	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\<*path*>
File (Windows XP)	%ALLUSERSPROFILE%\msd
File (other Windows)	%PROGRAMDATA%\msd

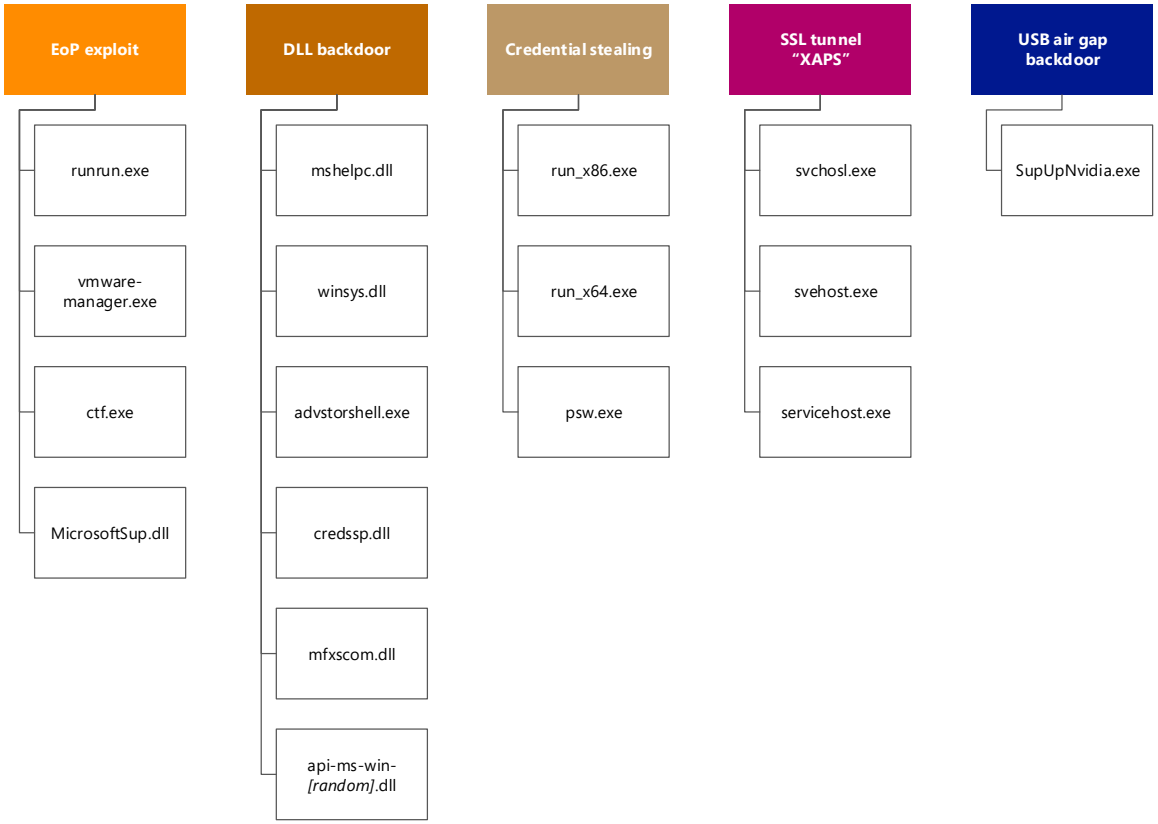
STRONTIUM ensures that its backdoor will run every time the computer starts by creating autostart extensibility point (ASEP) registry entries and shortcuts, which differ depending on what the attacker has chosen for the victim and which backdoor variant is used. (See "Advanced Malware Cleaning Techniques for the IT Professional" on page 96 of *Microsoft Security Intelligence Report, Volume 11 (January–June 2011)*, available from the Microsoft Download Center, for guidance on using Sysinternals tools to monitor ASEPs for signs of malware infection.) The most common ASEPs used by STRONTIUM for its malware include the following:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjectDelayLoad\
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
- HKEY_CURRENT_USER\Environment\UserInitMprLogonScript = <*batch file*>
- %ALLUSERSPROFILE%\Application Data\Microsoft\Internet Explorer\Quick Launch\
- %USERPROFILE%\Application Data\Microsoft\Internet Explorer\Quick Launch\

The STRONTIUM backdoor is composed of several pieces with different functions. The attacker can deploy a large set of tools to perform tasks including key logging, email address and file harvesting, information gathering about the local computer, and remote communication with C&C servers. STRONTIUM also uses a component that is designed to infect connected USB storage devices, so that information can be captured from *air-gapped* computers that are not on

the network when a user transfers the USB device to the air-gapped computer and then back to the network again.

Figure 9. Different types of STRONTIUM components and filenames used during recently observed incidents



The STRONTIUM group also appears to be active on non-Windows systems. Microsoft has seen solid indicators that STRONTIUM used malicious backdoors to take control of proxy servers, mail servers, and other systems running the Linux operating system. Microsoft also observed the group using domains that seem to be customized for different operating systems, including *mac.softupdates.info* and *linux.softupdates.info*. Although Microsoft does not generally study attacks on non-Windows systems, a multiplatform attack strategy is very much in line with what has been observed about STRONTIUM in general—that they have capabilities that cover a wide range of technologies—and any incident response against this adversary should take both Windows and non-Windows computers into consideration.

The STRONTIUM group also appears to be active on non-Windows systems.

Taking action

The STRONTIUM backdoor can communicate over different network protocols, including HTTP, SMTP, and POP3. Typically, the backdoor tests its connectivity with a series of HTTP POST requests to legitimate websites, and then establishes communication with its C&C servers. The domains STRONTIUM uses for its C&C servers are typically designed to avoid attracting attention if administrators notice them when reviewing network traffic, such as *softupdates.info* and *malwarecheck.info*, suggestive of software update and malware reputation services.

> The domains STRONTIUM uses are designed to avoid attracting attention.

In recent incidents during 2015, Microsoft observed STRONTIUM using a tunnel component designed to provide a remote encrypted interactive shell to a pre-configured IP address using proxy software on the victim's computer, such as the popular open-source Squid proxy. The tunneling module, which is customized for different targets, is slightly larger than 1 MB and is statically linked with an OpenSSL library. Based on debug information left in some samples, some researchers have reported that the name of the component may be "XAPS OBJECTIVE" or "XTUNNEL."[4] The C&C server for this tunnel could be either hardcoded in the binary or passed as a command-line parameter at startup.

Figure 10. "XAPS" in the STRONTIUM tunnel module binary

```
000F9ED0  00 00 00 00 2E 65 78 65 00 00 00 00 43 00 4F 00  .....exe....C.O.
000F9EE0  4E 00 49 00 4E 00 24 00 00 00 00 00 31 23 51 4E  N.I.N.$.....1#QN
000F9EF0  41 4E 00 00 31 23 49 4E 46 00 00 00 31 23 49 4E  AN..1#INF...1#IN
000F9F00  44 00 00 00 31 23 53 4E 41 4E 00 00 52 53 44 53  D...1#SNAN..RSDS
000F9F10  3C F3 97 0F AB 5B A3 47 93 2A 3C FE 9E 9A F8 2D  <ó—.«[£G"*<þžšø-
000F9F20  01 00 00 00 43 3A 5C 55 73 65 72 73 5C 55 73 65  ....C:\Users\Use
000F9F30  72 5C 44 65 73 6B 74 6F 70 5C 78 61 70 73 5F 74  r\Desktop\xaps_t
000F9F40  68 72 6F 75 67 68 5F 73 71 75 69 64 5F 64 65 66  hrough_squid_def
000F9F50  61 75 6C 74 5F 70 72 6F 78 79 5C 52 65 6C 65 61  ault_proxy\Relea
000F9F60  73 65 5C 58 41 50 53 5F 4F 42 4A 45 43 54 49 56  se\XAPS_OBJECTIV
000F9F70  45 2E 70 64 62 00 00 00 00 00 00 00 00 00 00 00  E.pdb...........
000F9F80  00 00 00 00 00 D0 4F 00 8C AF 4F 00 00 00 00 00  .....ÐO.Œ¯O.....
```

Samples for this component include the items in the following table:

[4] Gastbeitrag, "Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag," Netzpolitik.org, June 19, 2015, https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/.

Figure 11. Known samples for the STRONTIUM XAPS tunnelling component

MD5 hash	SHA-1 hash	File name
800af1c9d341b846a856a1e686be6a3e	0450aaf8ed309ca6baf303837701b5b23aac6f05	svehost.dll
9d86ba47a0b876cdc7fb0c9ad471cd67	64515c7ce8bcc656d54182675bd2d9ffceffe845	svchosl.exe
1957f5370d584a2acd74179340ef3005	3ec270193815fa2bd853ea251d93fdfffcbc40d6	svehost.exe
f5a54476d3d05c8f0804f3d2d5818928	e5039bb420f9a3a23aaa9ee7392bd05dfee42540	svehost.exe
4ac8d16ff796e825625ad1861546e2e8	1535d85bee8a9adb52e8179af20983fb0558ccb3	servicehost.exe

After gaining a foothold on one computer, STRONTIUM attempts to move laterally through the organization by compromising additional computers to gain access to more data and high-value targets. STRONTIUM uses publicly available tools such as WinExe (a remote command-line execution tool) and Mimikatz (a Windows credential gathering tool) to move between computers via methods such as Pass the Hash (PtH). In recent incidents Microsoft observed STRONTIUM using a customized version of Mimikatz that was recompiled with a privilege escalation exploit (CVE-2015-1701, addressed by Security Bulletin MS15-051) and stored captured credential information in a dedicated file, *pi.log*.

Figure 12. A customized version of Mimikatz storing passwords in the file *pi.log*

```
00401C77 ; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE
00401C77 _WinMain@16     proc near               ; CODE XREF: __
00401C77
00401C77 var_8           = byte ptr -8
00401C77 var_4           = byte ptr -4
00401C77 hInstance       = dword ptr  8
00401C77 hPrevInstance   = dword ptr  0Ch
00401C77 lpCmdLine       = dword ptr  10h
00401C77 nShowCmd        = dword ptr  14h
00401C77
00401C77                 push    ebp
00401C78                 mov     ebp, esp
00401C7A                 push    ecx
00401C7B                 push    ecx
00401C7C                 cmp     dword_446984, 1
00401C83                 push    ebx
00401C84                 mov     ebx, offset off_446478
00401C89                 jnz     short loc_401C92
00401C8B                 push    offset aPi_log  ; "pi.log"
00401C90                 jmp     short loc_401C9A
```

STRONTIUM has displayed an advanced understanding of military and classified government networks, and uses a component that is designed to extract information from air-gapped computers. This module registers a device callback

via RegisterDeviceNotification[5] and receives a notification every time a USB mass storage device is inserted into a compromised computer. Depending on the variant deployed, the backdoor may simply harvest the entire contents of the USB device and save it on the local computer for later extraction, or it may also use Autorun malware to transfer itself to the device so that it can attempt to compromise any other computers it is later inserted into, including air-gapped computers.[6]

Figure 13. The device notification routine registered by a STRONTIUM USB module

```
004021FC 74 6E                          jz      short loc_40226C
004021FE 2D 17 02 00 00                 sub     eax, 217h       ; WM_DEVICECHANGE ?
00402203 56                             push    esi
00402204 8B 75 14                       mov     esi, [ebp+lParam]
00402207 57                             push    edi
00402208 8B 7D 10                       mov     edi, [ebp+wParam]
0040220B 75 4B                          jnz     short defwndproc_and_exit
0040220D 81 FF 00 80 00 00              cmp     edi, 8000h      ; DBT_DEVICEARRIVAL
00402213 75 43                          jnz     short defwndproc_and_exit
00402215 83 7E 04 02                    cmp     dword ptr [esi+4], 2
00402219 75 3D                          jnz     short defwndproc_and_exit
0040221B 0F B7 46 10                    movzx   eax, word ptr [esi+10h]
0040221F 83 F8 01                       cmp     eax, 1
00402222 74 34                          jz      short defwndproc_and_exit
00402224 83 F8 02                       cmp     eax, 2
00402227 74 2F                          jz      short defwndproc_and_exit
00402229 8B 4E 0C                       mov     ecx, [esi+0Ch]
0040222C 32 C0                          xor     al, al
0040222E 8B FF                          mov     edi, edi
00402230
00402230                        loopDrives:                     ; CODE XREF: pfunc_Window+4B↓j
00402230 F6 C1 01                       test    cl, 1
00402233 75 08                          jnz     short loc_40223D
00402235 FE C0                          inc     al
00402237 D1 E9                          shr     ecx, 1
00402239 3C 1A                          cmp     al, 26          ; Z:\
0040223B 7C F3                          jl      short loopDrives
0040223D
0040223D                        loc_40223D:                     ; CODE XREF: pfunc_Window+43↑j
0040223D 8D 4D 0C                       lea     ecx, [ebp+Msg]
00402240 51                             push    ecx
00402241 04 41                          add     al, 'A'         ; Drive Letter
```

Some STRONTIUM victims have reported the presence of computers running Kali Linux on their networks. Kali Linux is a Linux distribution that combines a variety of tools for the purpose of penetration testing and security assessment. It contains tools for password attacks, sniffing & spoofing, maintaining access, hardware hacking, reverse engineering, information gathering, vulnerability analysis, wireless attacks, web application attacks, stress testing, and forensic and

[5] See msdn.microsoft.com/library/windows/desktop/aa363431%28v=vs.85%29.aspx for more information about this function.

[6] Changes to the way the AutoRun feature works make it more difficult for this technique to succeed in recent versions of Windows. See blogs.technet.com/b/security/archive/2011/06/27/defending-against-autorun-attacks.aspx for more information.

exploitation analysis. The tool lists within each category are quite extensive and the distribution is actively maintained, so that STRONTIUM can always take advantage of the latest open-source tools. STRONTIUM does not deploy this Linux distribution on an existing computer that belongs to the targeted institution; rather, it uses a VPN connection to join one of its own Kali Linux computers to the victim's network, possibly using the tunnel component that was previously deployed. This approach allows STRONTIUM to only ephemerally expose its toolset to the victim's network.

Guidance

STRONTIUM is a very challenging adversary for a targeted institution to defend against: it possesses a broad range of technical exploitation capabilities, significant access to resources such as previously undiscovered zero-day exploits, and the determination to keep up an attack for months or years until it succeeds. Nevertheless, there are steps an organization can take to significantly reduce its attack surface and decrease the probability of a successful compromise.

STRONTIUM is a challenging adversary for a targeted institution to defend against.

- Stay up-to-date on vendor security updates and deploy them quickly after they are released. All of the exploits discussed in this section have been addressed by security updates from Microsoft and other vendors. STRONTIUM depends heavily on the presence of out-of-date software installations inside target institutions, so keeping software up-to-date denies the group the use of some of its most effective tools.
- Take advantage of the mitigations built into your software. Recent versions of Windows and other software include critical mitigations that render many of STRONTIUM's exploits ineffective when deployed. Figure 5 on page 8 lists a number of zero-day exploits that STRONTIUM has used in recent campaigns. Most of these exploits will fail if tried on a computer running the latest versions of Windows and Office, even without security updates that address the vulnerabilities:
  - The STRONTIUM exploits that target CVE-2015-1641 and CVE-2015-2424, which affect Microsoft Word and have been addressed by Security Bulletins MS15-033 and MS15-070 respectively, depend on static hard-coded ROP chains that fail when address space layout randomization

(ASLR) is enabled. Office 2013 and Office 2016 both run with ASLR enabled by default, rendering these exploits ineffective.

Figure 14. Snippet of the ROP chain used in the CVE-2015-2424 exploit; it fails against Office installations with ASLR enabled

```
szMarker        db 't00tt00t'
ROP             dd 7C809AF1h            ; kernel32!VirtualAlloc
                dd 771463EAh            ; ret addr
                dd 0D10000h             ; lpAddress
                dd 200000h              ; dwSize 0x200000
                dd 3000h                ; flAllocationType = MEM_COMMIT|MEM_RESERVE
                dd 40h                  ; flProtect = PAGE_EXECUTE_READWRITE
NOP_PADDDING    dd 90909090h
                dd 90909090h
                dd 90909090h
                dd 90909090h
; ---------------------------------------------------------------------------

Shellcode_Start:
                jmp     fist_jump
; ---------------------------------------------------------------------------

get_poc:                                ; CODE XREF: seg000:fist_jump↓p
                pop     esi             ; ESI = 100147F
                xor     ebx, ebx
                mov     bl, 67h
                xor     ecx, ecx
                mov     ecx, 51h
                mov     edi, esi

loc_100146F:                            ; CODE XREF: seg000:01001473↓j
                lodsb
                xor     al, bl
                stosb
                loop    loc_100146F
                jmp     dec_fist_stage
```

- The exploit targeting CVE-2015-3043, a vulnerability in Adobe Flash Player addressed by Adobe Security Bulletin APSB15-06, fails in Internet Explorer running on an up-to-date installation of Windows 8.1 or Windows 10 because of Control Flow Guard, a mitigation introduced in a Windows 8.1 security update in November 2014. Control Flow Guard mitigates virtual function hijacking attempts such as the one involving the cancel() method shown in Figure 15.

Figure 15. Snippet from the STRONTIUM ActionScript exploit code targeting CVE-2015-3043 in Adobe Flash Player, which fails against CFG mitigation

```
_loc_9 = _loc_7 * 4;
_loc_10 = readVectorInt(varVectorPoisoned, 0, _loc_9 + 32);
_loc_6 = (_loc_10 - _loc_9) - 24;
addrOfShellcode = _loc_6 + this.intOff1000;
_loc_11 = readVectorInt(varVectorPoisoned, 0, _loc_9 + 16);
_loc_13 = findRopGadgets(varVectorPoisoned, _loc_6, _loc_11);
_loc_14 = _loc_13[0] + 8;
_loc_15 = _loc_13[1] + 8;

writeVectorInt(varVectorPoisoned, 0, _loc_9 + 16, _loc_6 + 16);
writeVectorInt(varVectorPoisoned, 0, 0, 4096);
writeVectorInt(varVectorPoisoned, 0, 4, addrOfShellcode);
writeVectorInt(varVectorPoisoned, 0, 16, _loc_15);
writeVectorInt(varVectorPoisoned, 0, 28, _loc_14);

//try to call corrupted function pointer to trigger RCE
k = 0;
while(k < (varArrFileRef.length - 1))
{
    varArrFileRef[k].cancel();
    k++;
}
```

- The kernel vulnerabilities exploited by STRONTIUM (CVE-2015-1701, addressed by Security Bulletin MS15-051, and CVE-2015-2387, addressed by Security Bulletin MS15-077) could not work in Windows 8 and newer platforms running on hardware that supports Supervisor Mode Execution Protection (SMEP) and other kernel mitigations.[7] In fact, the exploit is coded to abort execution if running on an operating system other than Windows 7.

[7] See "Exploit Mitigation Improvements in Windows 8" (https://media.blackhat.com/bh-us-12/Briefings/M_Miller/BH_US_12_Miller_Exploit_Mitigation_Slides.pdf) for more information.

Figure 16. STRONTIUM's CVE-2015-1701 exploit terminates execution on the newest versions of Windows

```
getOSversion:
                lea     eax, [ebp+VersionInformation]
                push    eax             ; lpVersionInformation
                mov     [ebp+VersionInformation.dwOSVersionInfoSize], 114h
                call    ds:GetVersionExW
                test    eax, eax
                jz      short exit_EAX_ZERO

checkOSversion:                         ; win 6.1 = WINDOWS 7
                cmp     [ebp+VersionInformation.dwMajorVersion], 6
                jnz     short exit_EAX_ZERO ; skip if Windows 8 or above
                cmp     [ebp+VersionInformation.dwMinorVersion], 1
                jnz     short exit_EAX_ZERO ; skip if Windows 8 or above

setupEPROCESSoffsets:
                push    esi
                mov     const_00000036, 36h
                mov     const_0000002C, 2Ch
                mov     const_00000040, 40h
                mov     const_000000F8, 0F8h
                call    getPSlookupAPI_from_ntoskrnl
                xor     esi, esi
                mov     PsLookupProcessByProcessId, eax ; EAX=kernel func
                cmp     eax, esi
                jnz     short continueExploitation
                xor     eax, eax
                jmp     short pop_and_exit
; ---------------------------------------------------------------------------

exit_EAX_ZERO:                          ; CODE XREF: runThreadWIN32k_EOP+2C↑j
                                        ; runThreadWIN32k_EOP+35↑j ...
                xor     eax, eax
                jmp     short exit
```

- Enforce segregation of privileges on user accounts and apply all possible safety measures to protect Admin accounts from being compromised; STRONTIUM relies on pass-the-hash techniques and elevation of privileges to successfully move laterally across networks. See "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft, Version 2," available at the Microsoft Download Center, for more information.
- In enterprise environments in which isolated computer networks (air-gapped) and Internet connected networks co-exist, enforce strong policies to prevent sharing and usage of removable media across the air gap.
- Conduct enterprise software security awareness training, and build awareness about malware infection prevention. STRONTIUM heavily relies on social engineering to entice individual targets into clicking links to malware. Security training can raise awareness around this attack vector.
- Institute multi-factor authentication. As STRONTIUM extensively uses credential-stealing spear phishing attacks, multi-factor authentication can be an effective tool to prevent unauthorized access even if credentials are stolen.

- Prepare your network to be forensically ready, so that you can achieve containment and recovery if a compromise occurs. A forensically ready network that records authentications, password changes, and other significant network events can help to quickly identify affected systems.
- Keep personnel and personal data private. STRONTIUM uses open-source intelligence (OSINT) to obtain its initial lists of victims, which might include things like name and email address, but can expand into employment information and other items of interest. These are all pieces of information STRONTIUM can use to devise a realistic attack. The more information STRONTIUM has available, the better they can target you. Make sure your email is kept confidential and privacy settings on social media don't disclose sensitive information publicly.

Focus on Brazil:

Win32/Banload and Banking Malware

Online banking is big business in Brazil, where more than half of all banking transactions have been made using Internet-connected devices in recent years.[8] Unfortunately, the popularity of online banking in Brazil has drawn the attention of criminals, who have made the country a world capital for banking malware for the last several years.

Win32/Banload, the most commonly encountered malware family in Brazil in 2Q15, is a generic detection for threats that download malware designed to steal banking credentials, which themselves are usually identified as other threats. (Encounter rates for these related threats are generally much lower than for Banload, in part because Microsoft real-time security products block Banload variants before they can download additional malware; therefore, examining Banload encounter rates is a useful proxy for understanding the banking malware problem in general.) Together, Banload and its related families have been a major part of the malware problem in Brazil for nearly ten years.

Criminals have made Brazil a world capital for banking malware for the last several years.

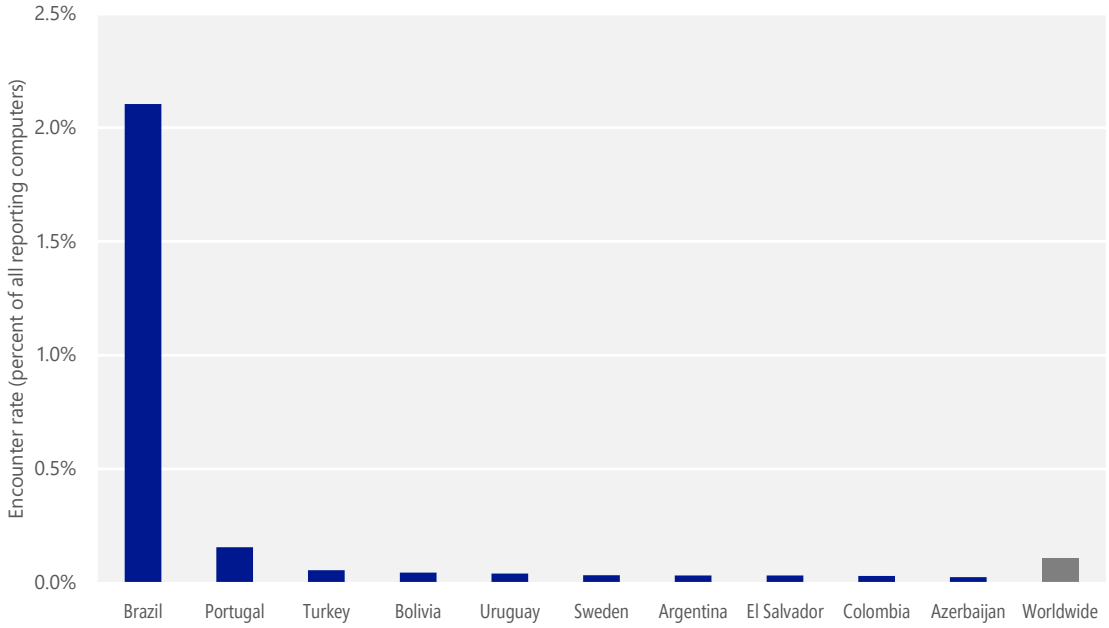
Distribution and trends

Although some variants have been found to target banks elsewhere, Banload remains an almost exclusively Brazilian threat. More than 93 percent of Banload encounters in 2Q15 occurred in Brazil, and the encounter rate for Banload in Brazil was 2.1 percent in 2Q15, compared to 0.16 percent in Portugal, the location with the second highest Banload encounter rate. While Banload was the

[8] Michael Oleaga, "Online Banking Growing in Brazil: More Than Half Made Digital Transactions in 2013," *Latin Post*, April 2, 2014, http://www.latinpost.com/articles/9959/20140402/online-banking-growing-brazil-more-half-made-digital-transactions.htm.

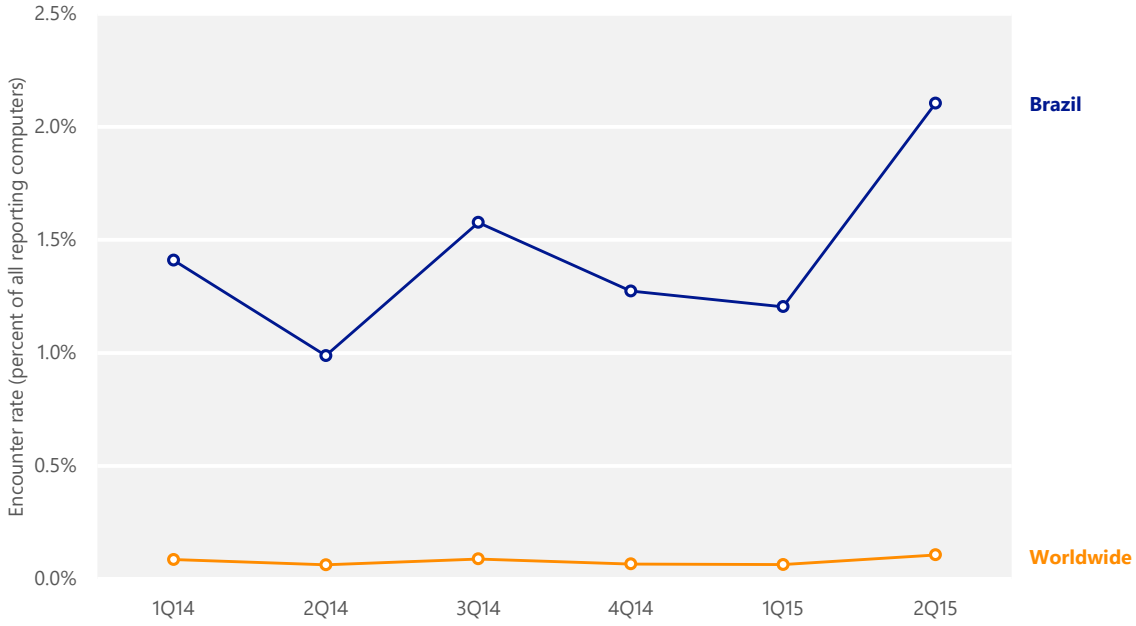
most commonly encountered threat family in Brazil in 2Q15, it ranked just 39th worldwide.

Figure 17. The top ten countries/regions encountering Win32/Banload in 2Q15



Banload has consistently been encountered at much higher rates in Brazil than in the rest of the world. Over the past six quarters the encounter rate for Banload in Brazil has fluctuated between 1.0 percent and 2.1 percent, while the worldwide Banload encounter rate has ranged between 0.06 percent and 0.11 percent. Despite a generally rising trend that accelerated in 2Q15, the fluctuations shown in Figure 18 are fairly typical for Banload and do not necessarily presage significantly increased encounter rates in the future.

Figure 18. Banload encounter rate trends worldwide and in Brazil, 1Q14–2Q15



Propagation and technical details

Threats detected as Banload are created and distributed by many different parties, who may have little or no connection to each other. Most variants operate in similar ways. Banload might be installed by other malware, or use social engineering to trick the user into launching it. After it is installed, it contacts a remote host and downloads additional files, which then attempt to steal banking credentials and transmit them back to the attacker. Banload variants have been observed to connect to many different remote hosts, including malicious sites as well as legitimate sites that have been compromised. As with many other malware families, the hosts are not confined to any particular region; attackers typically establish malicious hosts wherever a vulnerable server can be found to compromise.

> Many Banload variants attempt to disable security products installed on the computer.

Some Banload variants check the configured system language upon installation and only download additional files if it is set to Portuguese. Although Banload usually does not attempt to steal banking credentials itself, many variants transmit other details about the computer environment to the attacker, such as the computer name, user name, and Windows version.

Many Banload variants attempt to disable security products installed on the computer, including G-Buster Browser Defense, a browser add-on that many large Brazilian banks provide to their customers to protect banking sessions from malware. Some variants modify the registry so that Banload will automatically launch each time the computer is started.

Win32/Banker and credential stealers

The malware threats downloaded by Banload variants are often detected as Win32/Banker and Win32/Bancos. Banker and Bancos are generic detections for data-stealing trojans that capture online banking credentials, such as account names and passwords, and relay the captured information to a remote attacker. As with Banload, these threats are created by many different people who often have no connection to each other apart from their common purpose of stealing banking credentials. Banker and Bancos variants typically monitor browser activity for banking sessions involving large and well-known Brazilian banks, including:

- Banco Bradesco (*bradesco.com.br*)
- Banco do Brasil (*bb.com.br*)
- Banco do Estado do Rio Grande do Sul (*banrisul.com.br*)
- Banco Itaú (*itau.com.br*)
- Banco Safra (*safra.com.br*)
- Banco Santander (*santander.com.br*)
- Caixa Econômica Federal (*caixa.gov.br*)
- Citibank (*citibank.com.br*)
- HSBC (*hsbc.com.br*)

As with Banload, many Banker and Bancos variants attempt to disable security products installed on the computer, including G-Buster Browser Defense, and modify the registry so the malware will automatically launch each time the computer is started.

Win32/BrobanDel and boleto malware

Another type of banking malware that has affected Brazil recently targets *boletos bancários*, a popular payment method there. A boleto bancário, usually simply called a boleto, is a payment order generated by a merchant or other

payee, similar to an invoice. Boletos are popular in Brazil because they provide a mechanism for people to pay bills or other debts without having a bank account; they can be paid in cash at a wide range of locations, including banks, post offices, and supermarkets. In recent years, online boletos have become popular: payers receive them over the Internet and can either pay them electronically from a bank account or can print them out for payment like conventional paper boletos. It is these online boletos that have been targeted by a new type of banking malware.

Figure 19. An example of a boleto bancário, a popular method of payment in Brazil

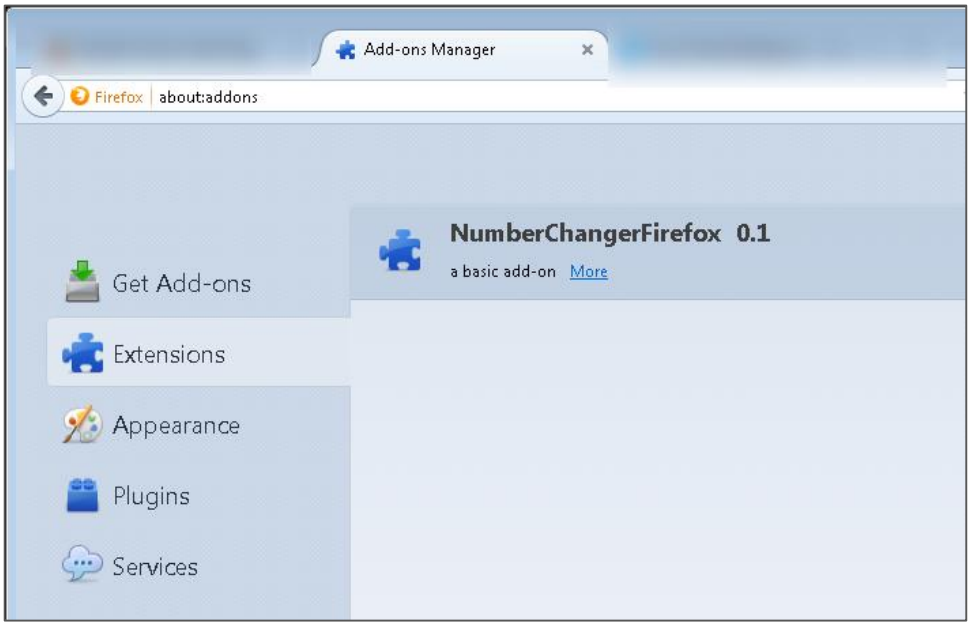
Itaú Banco Itaú S.A. | 341-7 | 34191.75009 00363.482936 81364.350009 6 63820000207900

Local de Pagamento: **Até o vencimento, preferencialmente no Itaú** **Após o vencimento, somente no Itaú**					Vencimento: **29/03/2015**
Cedente: **ARVATO SERVICOS, COMERCIO E INDUSTRIA GRAFICA LTDA CNPJ: 04.606.776/0002-91**					Agência/Código Cedente: **2938/13643-5**
Data Documento: **23/03/2015**	Número do Documento: **MS-BR-S-200004203**	Espécie Doc.: **RC**	Aceite: **N**	Data Processamento: **23/03/2015**	Nosso Número: **175/00003634-8**
Uso do Banco	Carteira: **175**	Espécie: **R$**	Quantidade	(x) Valor	(=) Valor do Documento: **2.079,00**
Instruções (Todas as informações deste bloqueto são de exclusiva responsabilidade do Cedente) Essa opção gera um boleto, que deve ser impresso e pago na agência bancária de sua preferência ou pela internet. Não faça depósito ou transferência entre contas. Se o boleto não for pago até o vencimento, o pedido será automaticamente cancelado. O banco confirmará o pagamento em até 3 (três) dias úteis após o pagamento. ATENÇÃO: O prazo de entrega será considerado somente após a confirmação do pagamento pela Instituição Financeira e liberação de seu pedido.					(-) Desconto (+) Mora/Multa (+) Outros Acréscimos (=) Valor Cobrado
Sacado **Johan** [redacted]					**CPF: 46** [redacted] **3**
Sacador/Avalista					**Ficha de Compensação**

Autenticação Mecânica

Every boleto has a unique identification number that specifies the bank, payee, and amount to be paid, among other information. The identification number is printed at the top of the boleto and encoded as a barcode at the bottom. A typical boleto malware variant (often detected as Win32/BrobanDel) installs itself as a browser add-on and monitors webpages for patterns that match a boleto. When it identifies a boleto, it alters the identification number so that when the recipient pays it, the money will be paid into an account controlled by the attacker, rather than the payee's account. The malware may re-encode the barcode to match the altered number, or simply corrupt it so that it cannot be optically scanned, requiring the cashier to enter the identification number by hand.

Figure 20. A malicious extension installed by Win32/BrobanDel to detect and alter boletos



New variants of Banload and the other families discussed in this section are discovered every day, and variants discovered in the future may exhibit different behaviors than those described here. Visit the Microsoft Malware Protection Center encyclopedia at https://www.microsoft.com/mmpc for the latest information about this and other threats.

Guidance

Effectively protecting users from malware requires an active effort on the part of organizations and individuals. For in-depth guidance, see "Top security solutions" at the Microsoft Malware Protection Center website at www.microsoft.com/mmpc.

Specific steps that IT administrators and individual users can take to protect themselves from malware include the following:

- Install security updates for all software as soon as is practical. Promptly installing security updates remains one of the best ways to defend against newly discovered threats.
- Configure computers to use Microsoft Update rather than Windows Update to automatically receive updates for a wide range of Microsoft products. Ensure that security updates from other software vendors are distributed automatically when possible.

- Install a comprehensive, real-time antimalware product from a reputable vendor on all of your organization's computers, and ensure that they receive frequent, regular definition or signature file updates.
- Take advantage of advanced Windows security features such as User Account Control and AppLocker to prevent unauthorized programs from running without permission.
- Use caution when clicking links to webpages and when opening attachments to email messages.
- Use a web browser such as Internet Explorer or Microsoft Edge that offers advanced protection against phishing and malicious webpages.

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security