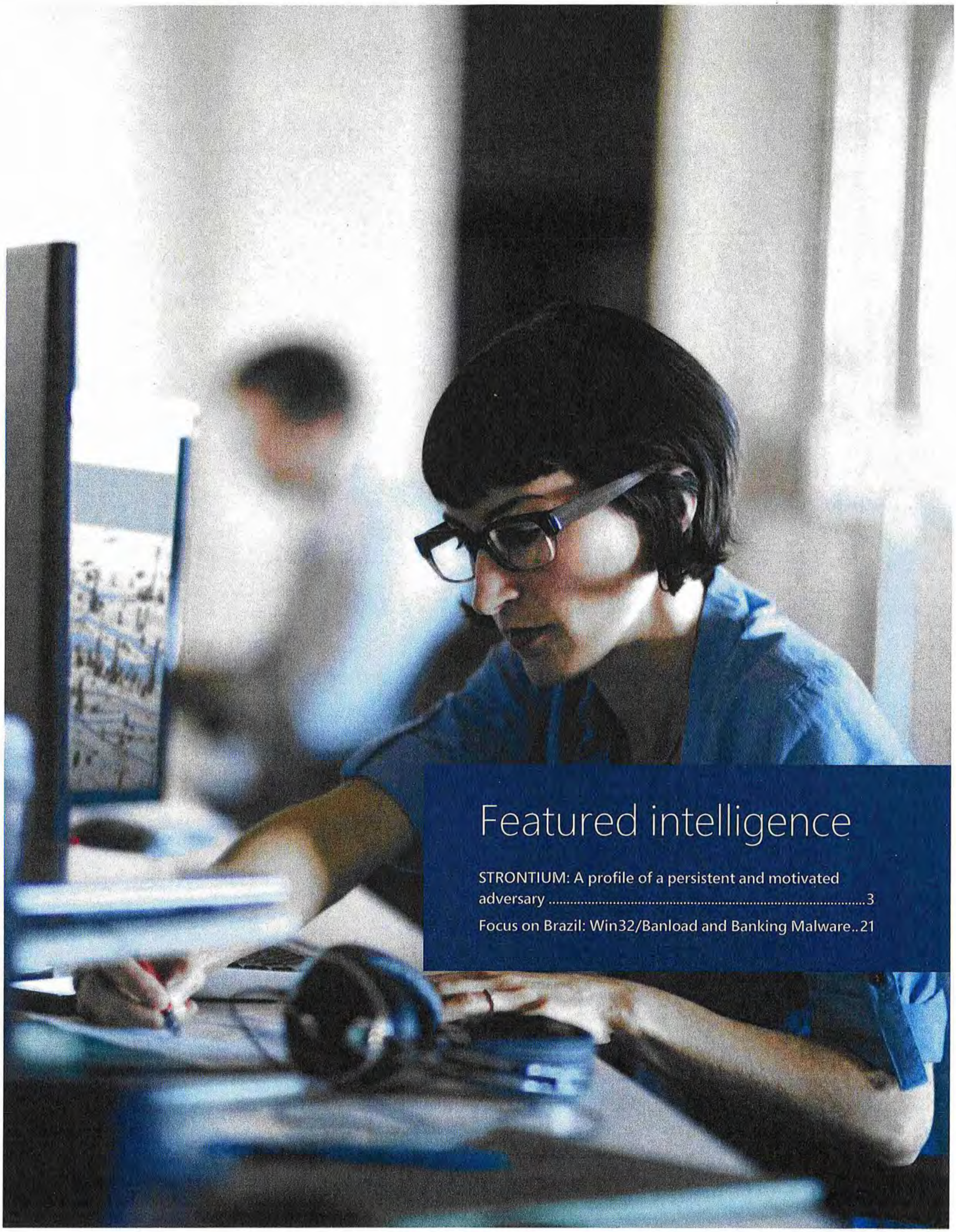
EXHIBIT 2

Microsoft Security Intelligence Report

Volume 19 | January through June, 2015



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.

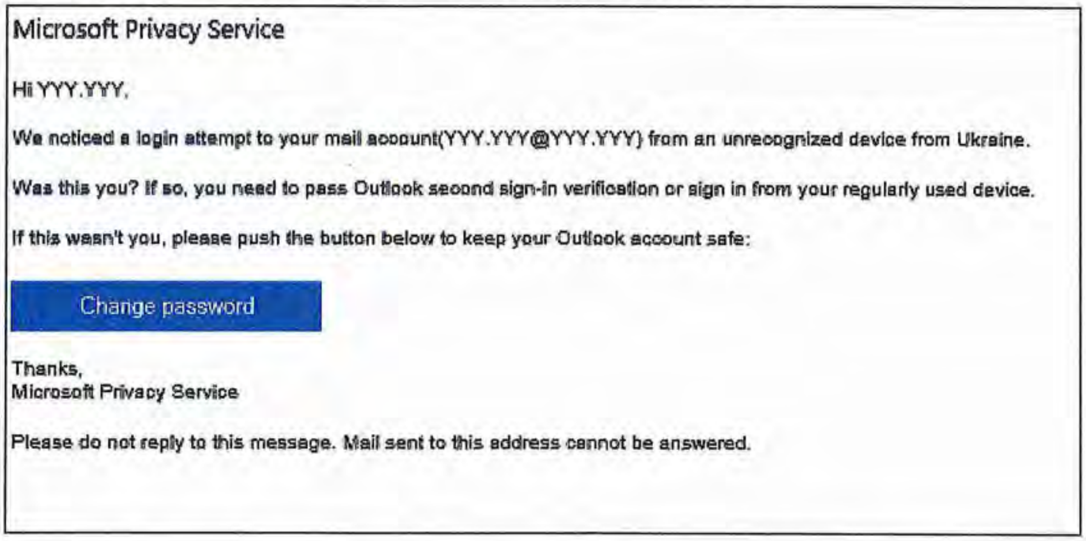
Reconnaissance and target identification

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



Microsoft Privacy Service

Hi YYY.YYY,

We noticed a login attempt to your mail account(YYY.YYY@YYY.YYY) from an unrecognized device from Ukraine.

Was this you? If so, you need to pass Outlook second sign-in verification or sign in from your regularly used device.

If this wasn't you, please push the button below to keep your Outlook account safe:

Thanks,
Microsoft Privacy Service

Please do not reply to this message. Mail sent to this address cannot be answered.

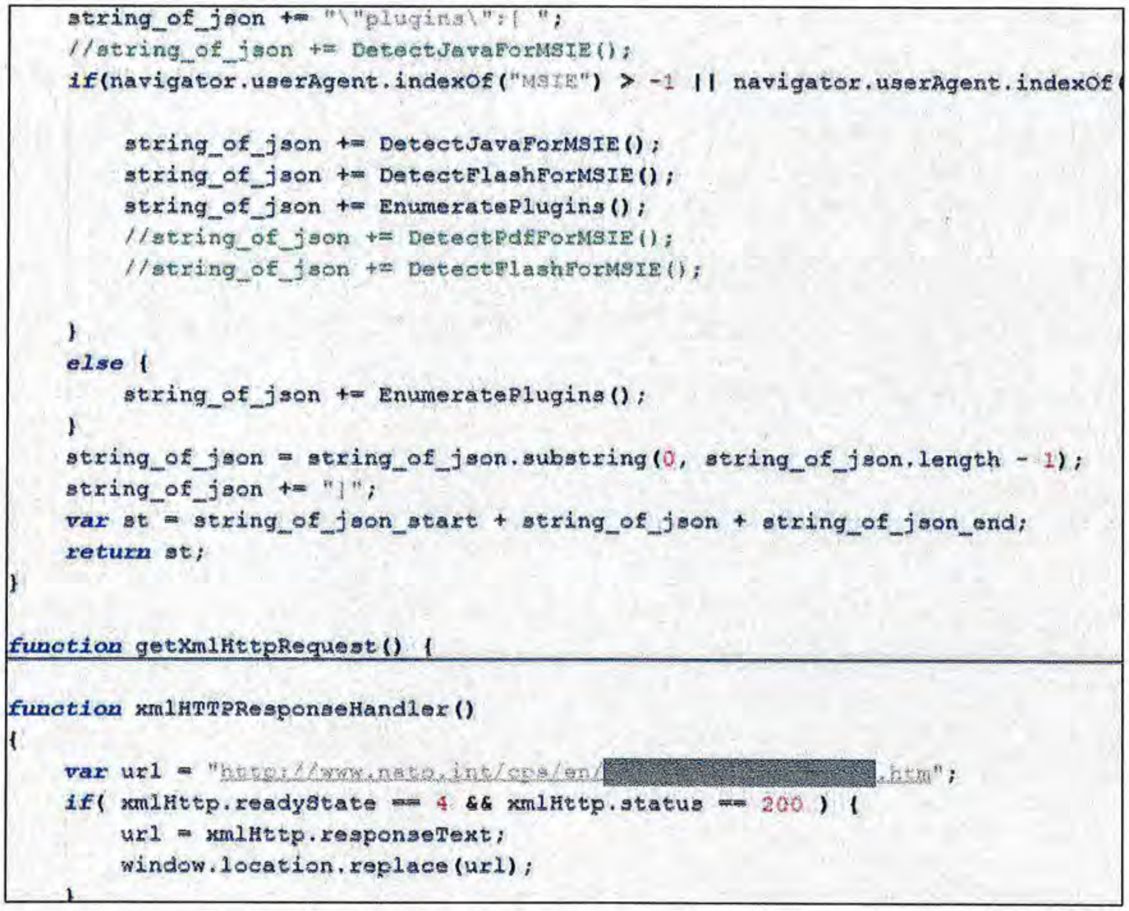
Typically, the link will lead to a domain name that is similar to a legitimate domain name used by the service in an effort to fool the user into thinking the message is legitimate. Figure 2 lists some examples.

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

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

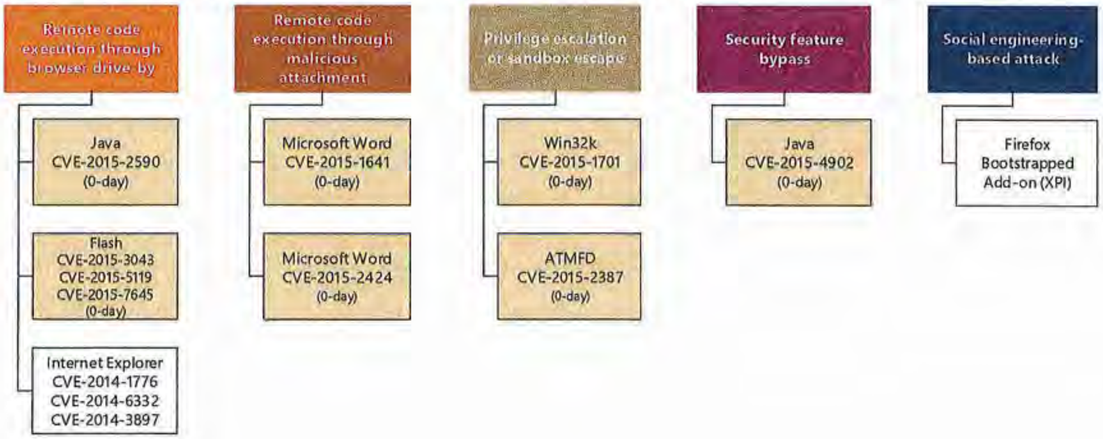
Zero-day exploits—exploits that target vulnerabilities for which the affected software vendor has not yet released a security update—form a significant part of STRONTIUM's arsenal. It is not yet clear whether the group researches vulnerabilities and develops the exploits themselves, or purchases them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

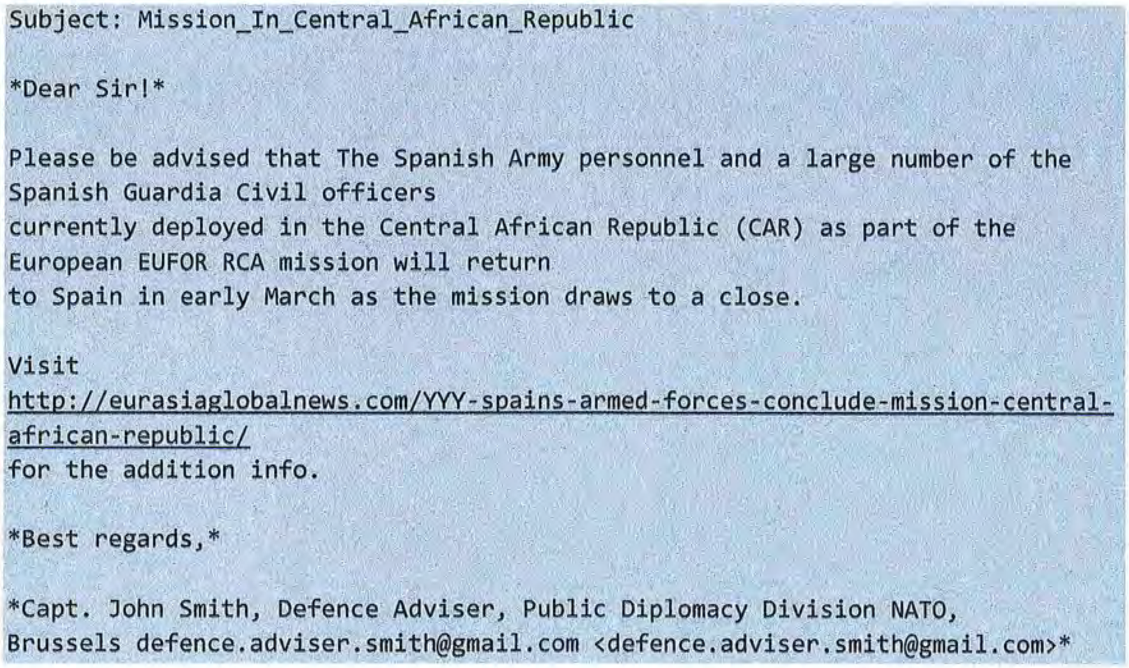
Figure 5. Some of the exploits used by STRONTIUM in attack campaigns in 2014 and 2015



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



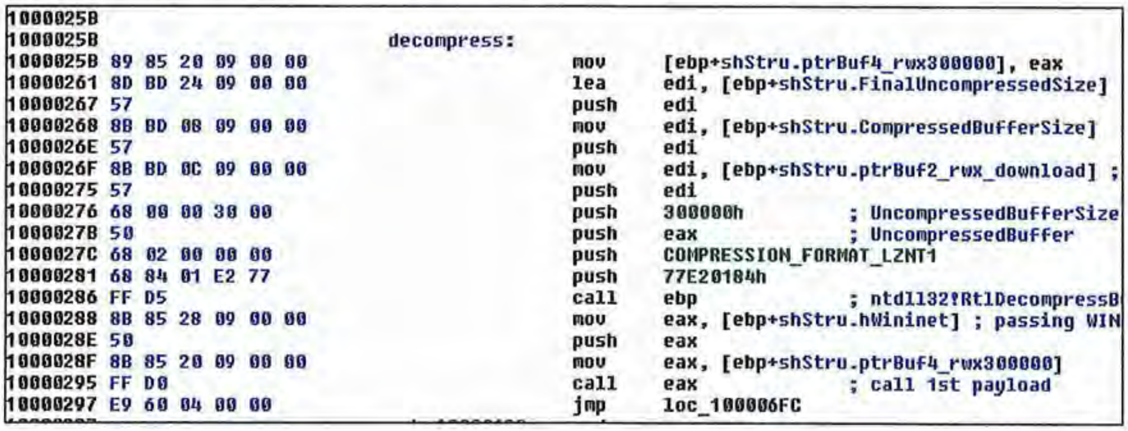
```
Subject: Mission_In_Central_African_Republic

*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, 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)

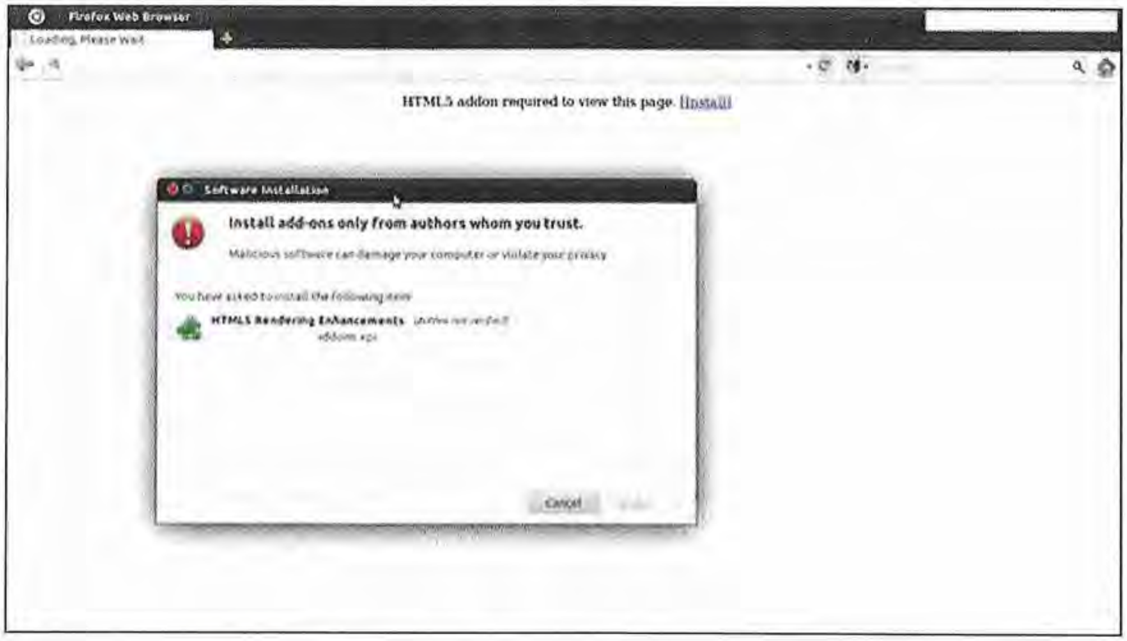
Figure 6. In-memory decompression and execution of remote payloads performed by STRONTIUM shellcode



```
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



HTML5 addon required to view this page. [Install]

Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy

You have asked to install the following item:

HTML5 Rendering Enhancements *(Author not verified)*
addons.xpi

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

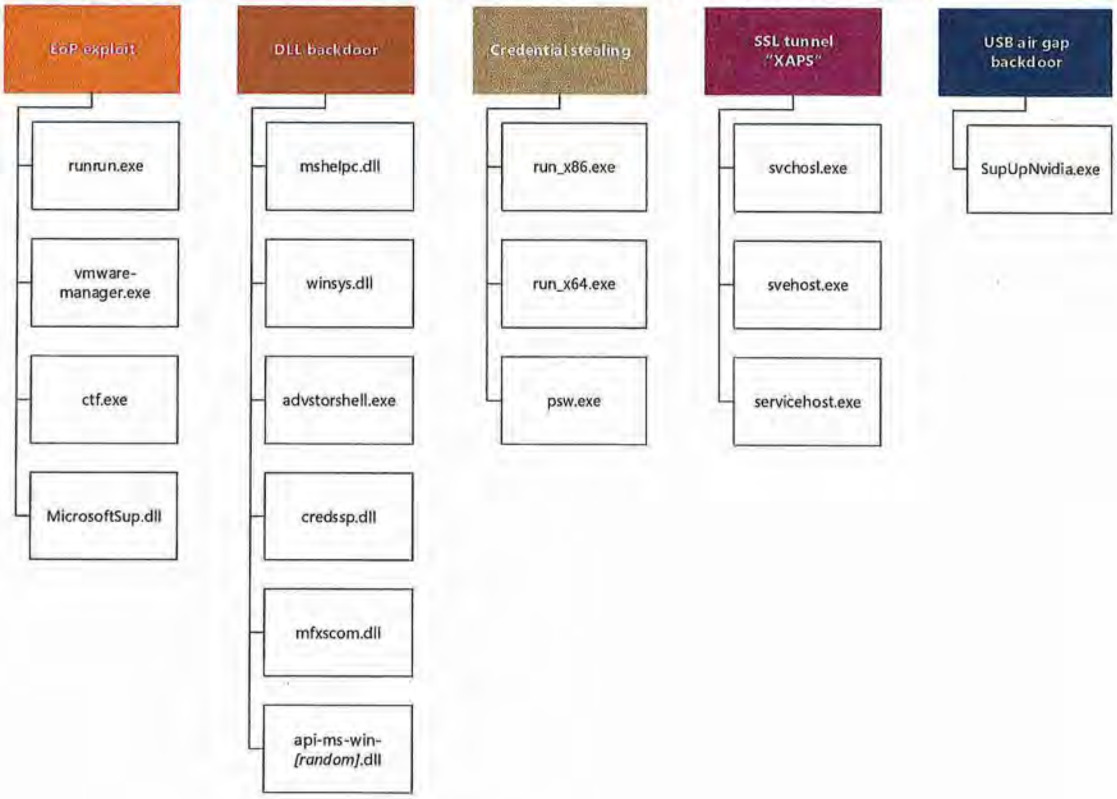
Format	Path
Registry	HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Explorer\<*path*>
File (Windows XP)	%ALLUSERSPROFILE%\msd
File (other Windows)	%PROGRAMDATA%\msd

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.

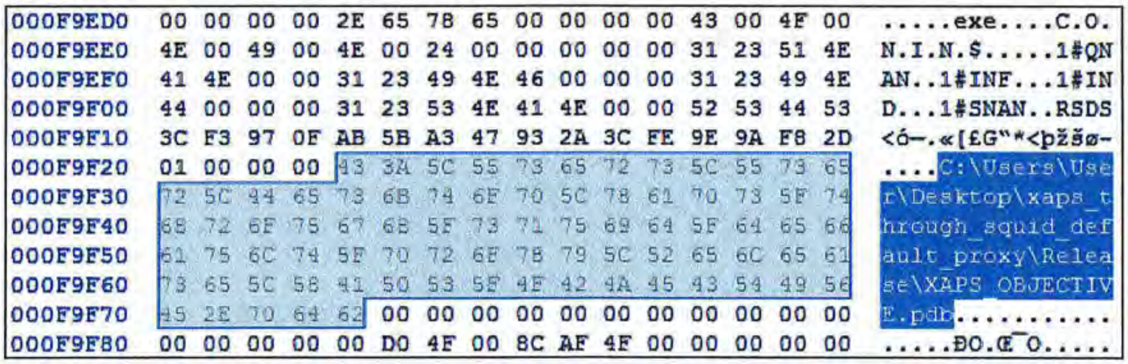
Taking action

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:

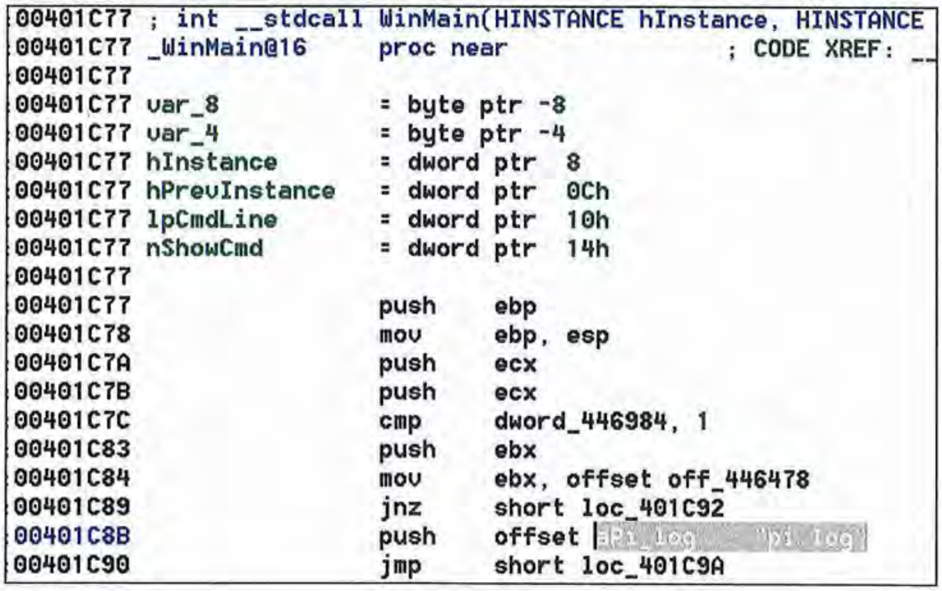
[4] Gastbeitrag, "Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag," Netzpolitik.org, June 19, 2015, https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-hack-of-the-left-party-infrastructure-in-bundestag/.

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*.

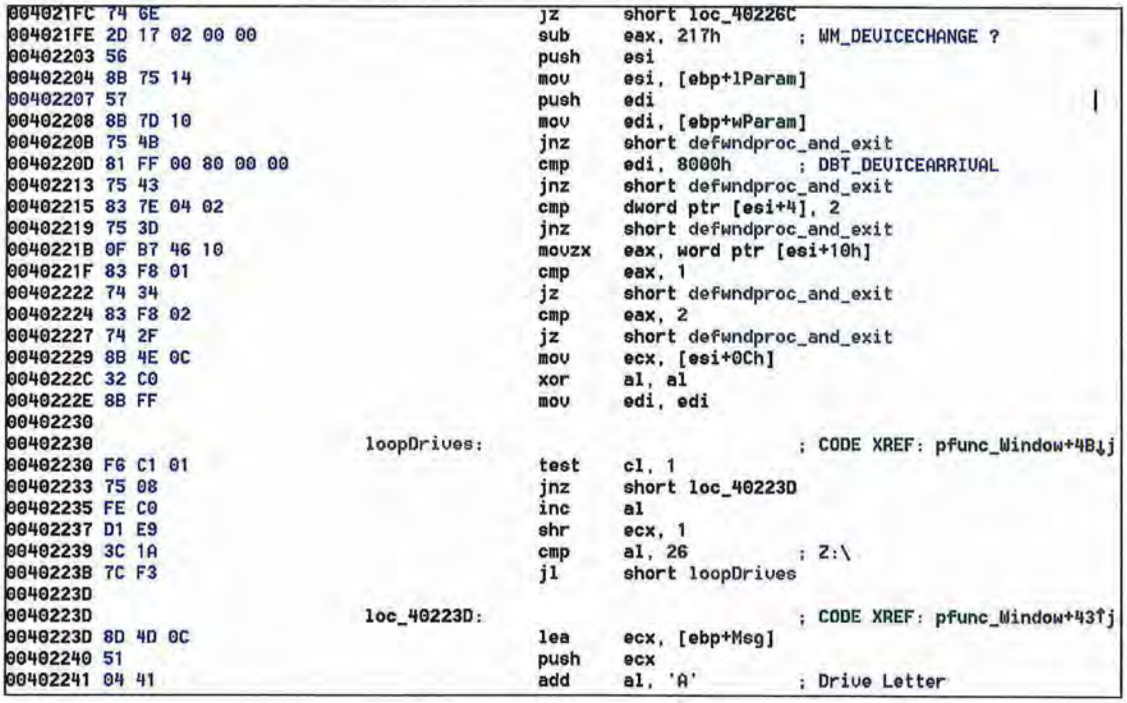
Figure 12. A customized version of Mimikatz storing passwords in the file *pi.log*



```
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

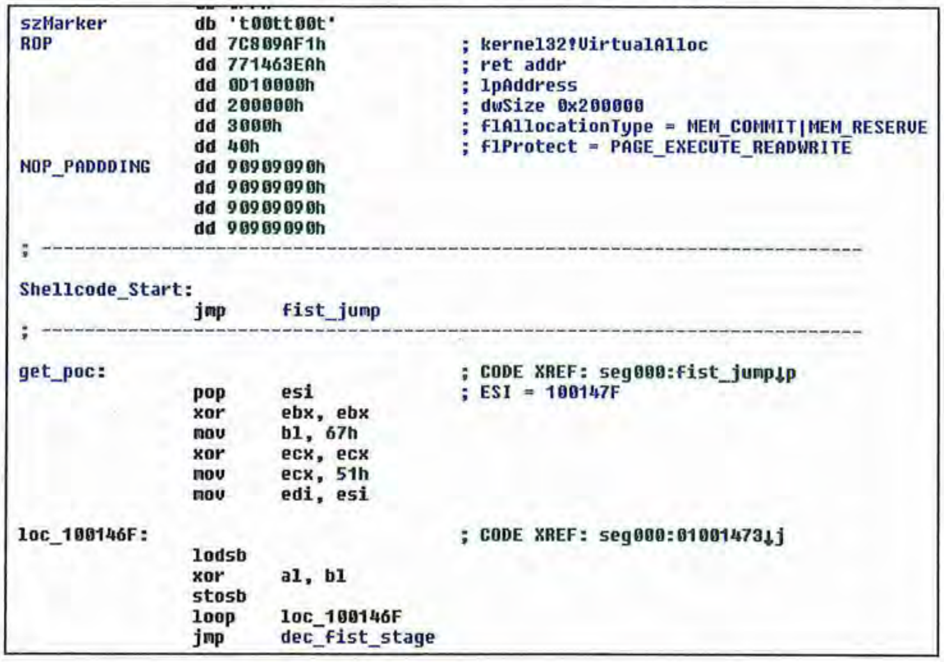
STRONTIUM is a very challenging adversary for a targeted institution to defend against: it possesses a broad range of technical exploitation capabilities, significant access to resources such as previously undiscovered zero-day exploits, and the determination to keep up an attack for months or years 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.

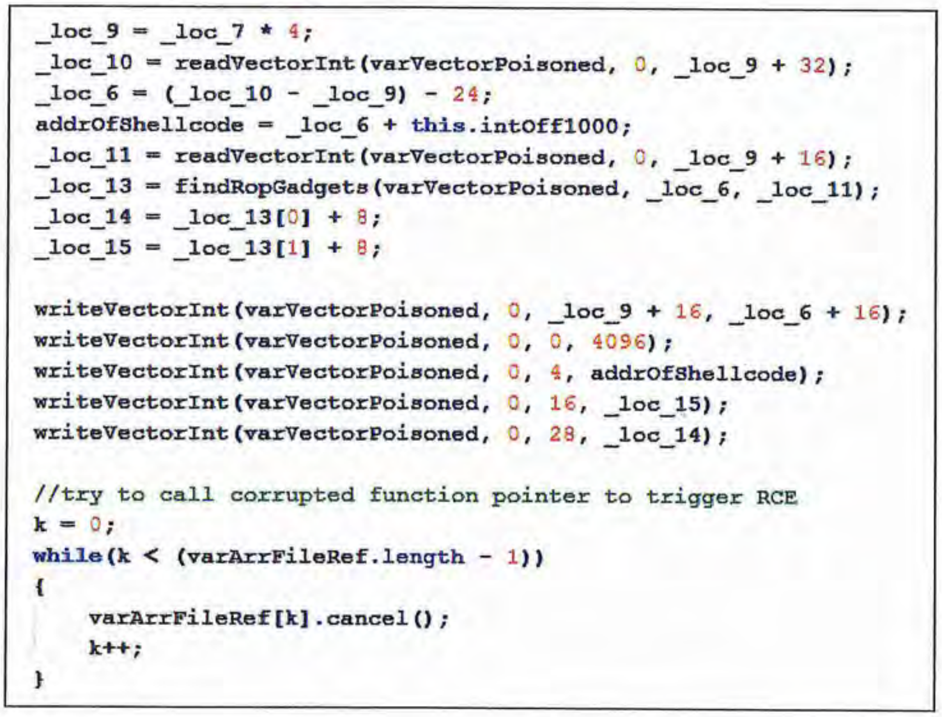
Figure 14. Snippet of the ROP chain used in the CVE-2015-2424 exploit; it fails against Office installations with ASLR enabled



```
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

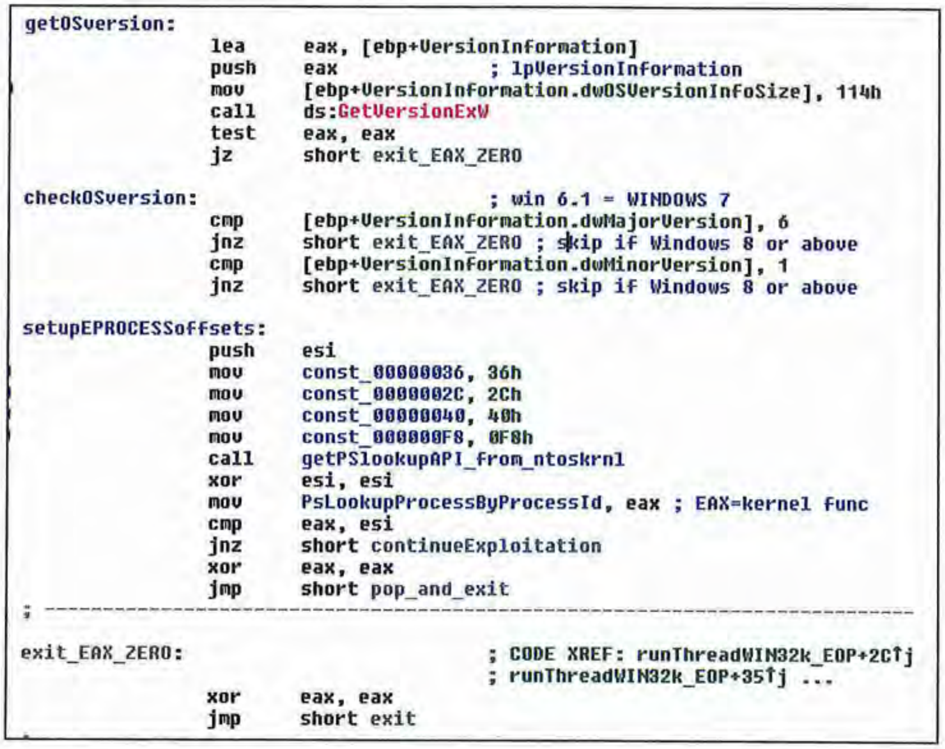


```
_loc_9 = _loc_7 * 4;
_loc_10 = readVectorInt(varVectorPoisoned, 0, _loc_9 + 32);
_loc_6 = (_loc_10 - _loc_9) - 24;
addrOfShellcode = _loc_6 + this.intOff1000;
_loc_11 = readVectorInt(varVectorPoisoned, 0, _loc_9 + 16);
_loc_13 = findRopGadgets(varVectorPoisoned, _loc_6, _loc_11);
_loc_14 = _loc_13[0]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