Microsoft

Microsoft Security Intelligence Report

Volume 21 | January through June, 2016

PROMETHIUM and NEODYMIUM: Parallel zero-day attacks targeting individuals in Europe

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Copyright © 2016 Microsoft Corporation. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Authors

Charlie Anthe
Cloud and Enterprise Security

Evan Argyle
Windows Defender Labs

Eric Douglas
Windows Defender Labs

Sarah Fender
Azure Security

Elia Florio
Windows Defender Labs

Chad Foster
Bing

Ram Gowrishankar
Windows Defender Labs

Volv Grebennikov
Bing

Paul Henry
Wadeware LLC

Aaron Hulett
Windows Defender Labs

Ivo Ivanov
Windows Defender Labs

Michael Johnson
Windows Defender Labs

Jeff Jones
Corporate Communications

Tim Kerk
Windows Defender Labs

Mathieu Letourneau
Windows Defender Labs

Marianne Mallen
Windows Defender Labs

Matt Miller
Microsoft Security Response Center

Chad Mills
Safety Platform

Nam Ng
Enterprise Cybersecurity Group

Hamish O'Dea
Windows Defender Labs

James Patrick Dee
Windows Defender Labs

Siddharth Pavithran
Windows Defender Labs

Daryl Pecelj
Microsoft IT Information Security and Risk Management

Ferdinand Plazo
Windows Defender Labs

Tim Rains
Commercial Communications

Paul Rebriy
Bing

Karthik Selvaraj
Windows Defender Labs

Tom Shinder
Azure Security

Nitin Sood
Windows Defender Labs

Tomer Teller
Azure Security

Vikram Thakur
Windows Defender Labs

Contributors

Eric Avena
Windows Defender Labs

Iaan D'Souza- Wiltshire
Windows Defender Labs

Dustin Duran
Windows Defender Labs

Tanmay Ganacharya
Windows Defender Labs

Chris Hallum
Windows and Devices Group

Satomi Hayakawa
CSS Japan Security Response Team

Sue Hotelling
Windows and Devices Group

Yurika Kakiuchi
CSS Japan Security Response Team

Louie Mayor
Windows Defender Labs

Dolcita Montemayor
Windows Defender Labs

Heike Ritter
Windows and Devices Group

Norie Tamura
CSS Japan Security Response Team

Steve Wacker
Wadeware LLC

David Weston
Windows Defender Labs

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 2016, 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, 1H16 represents the first half of 2016 (January 1 through June 30), and 4Q15 represents the fourth quarter of 2015 (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 135 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 and cloud-based detections. For the purposes of this report, a threat is defined as a malicious or unwanted software family or variant that is detected by the Microsoft Malware Protection Engine.

How to use this report

The *Microsoft Security Intelligence Report* has been released twice a year since 2006. Each volume is based upon data collected from millions of computers all over the world, which not only provides valuable insights on the worldwide threat landscape, both at home and at work, but also provides detailed information about threat profiles faced by computer users in more than a hundred individual countries and regions.

To get the most out of each volume, Microsoft recommends the following:

Read

Each volume of the report consists of several parts. The primary report typically consists of a worldwide threat assessment, one or more feature articles, guidance for mitigating risk, and some supplemental information. A summary of the key findings in the report can be downloaded and reviewed separately from the full report; it highlights a number of facts and subjects that are likely to be of particular interest to readers. The regional threat assessment, available for download and in interactive form at www.microsoft.com/security/sir/threat, provides individual summaries of threat statistics and security trends for more than 100 countries and regions worldwide.

Reading the volume in its entirety will provide readers with the most benefit and context, but the report is designed to provide value in small doses as well. Take a few minutes to review the summary information to find the information that will be of most interest to you and your organization. Consult the table of contents and the index to learn more about particular topics of interest.

Share

Microsoft also encourages readers to share each released volume, or its download link, with co-workers, peers, and friends with similar interests. The *Microsoft Security Intelligence Report* is written to be useful and accessible to a wide range of audiences. Each volume contains thousands of hours of research disseminated in easy to understand language, with advanced technical jargon kept to a minimum. Each section and article is written and reviewed to provide the most value for the time it takes to read.

Assess your own risk

Reading about the threats and risks that affect different types of environments presents a good opportunity to assess your own risks. Not every computer and entity faces the same risk from all threats. Assess your own risks and determine which topics and information can help you to best defend against the most significant risks.

The volume and scope of threats facing the typical organization make it important to prioritize. The greatest risk to any computer or organization is posed by currently and recently active threats. Pay attention to the threats that have most commonly affected your region or industry, focusing particularly on the most common successful attacks in the wild that cause the most problems. Give less consideration to very rare or theoretical-only attacks, unless your computers are at particular risk for such threats.

Educate

Microsoft strives to make this report one of the most valuable sources of threat and mitigation information that you can read and share. We encourage you to use the *Microsoft Security Intelligence Report* as a guide to educate your employees, friends, and families about security-related topics.

Anyone, including a business, may link, point to, or re-use articles in the *Microsoft Security Intelligence Report* for informational purposes, provided the material is not used for publication or sale outside of your company and you comply with the following terms: You must not alter the materials in any way. You must provide a reference to the URL at which the materials were originally found. You must include the Microsoft copyright notice followed by "Used with permission from Microsoft Corporation." Please see Use of Microsoft Copyrighted Content for further information.

Ask questions

Contact your local Microsoft representative with any questions you have about the topics and facts presented in this report. We hope that each volume provides a good educational summary and helps promote dialog between people trying to best secure their computing devices. Thank you for trusting Microsoft to be your partner in the fight against malware, hackers, and other security threats.

Featured intelligence

PROMETHIUM and NEODYMIUM: Parallel zero-day attacks targeting individuals in Europe

Windows Defender ATP

Microsoft proactively monitors the threat landscape for emerging threats. Part of this job involves observing the activities of targeted activity groups, which are often the first ones to introduce new exploits and techniques that are later used by other attackers. The previous two volumes of the *Microsoft Security Intelligence Report* explored the activities of two such groups, code-named STRONTIUM and PLATINUM, which used previously unknown vulnerabilities and aggressive, persistent techniques to target specific individuals and institutions—often including military installations, intelligence agencies, and other government bodies.

This volume chronicles two activity groups, code-named PROMETHIUM and NEODYMIUM, both of which target individuals in a specific area of Europe. Although most malware today either seeks monetary gain or conducts espionage for economic advantage, both of these activity groups appear to seek information about specific individuals.

In May 2016, both PROMETHIUM and NEODYMIUM were observed to launch attack campaigns. These campaigns used completely distinct infrastructure and primary malware, which indicated a lack of association at the operational level. However, the similarity in the campaigns' victim locale, timing, and use of the same zero-day exploit prior to public disclosure strongly indicates that the activity groups may be related at a higher organizational tier.

Microsoft is sharing information about these groups to raise awareness of their activities, and to help individuals and organizations implement existing mitigation options that significantly reduce risk from these attack groups and other similar groups.

Activity Group Profile: PROMETHIUM

Campaign summary: PROMETHIUM is an activity group that has been active since at least 2012. In 2016, an attack campaign by this group was recorded in early May that made use of an exploit for CVE-2016-4117, a vulnerability in Adobe Flash Player, which at the time was both unknown and unpatched. Adobe promptly and publicly acknowledged the zero-day vulnerability and pushed a security update.

PROMETHIUM and NEODYMIUM both target individuals in a specific area of Europe.

The attack itself began with certain individuals receiving links in instant messenger clients. These links led to malicious documents that invoked exploit code and eventually executed a piece of malware called Truvasys on unsuspecting victims' computers.

Administrators and users wondering whether they were targeted by PROMETHIUM can scan their network by using the indicators listed in the appendix, by using Windows Defender to examine their logs for "Truvasys," or by searching for PROMETHIUM in their Windows Defender Advanced Threat Protection product console alerts.

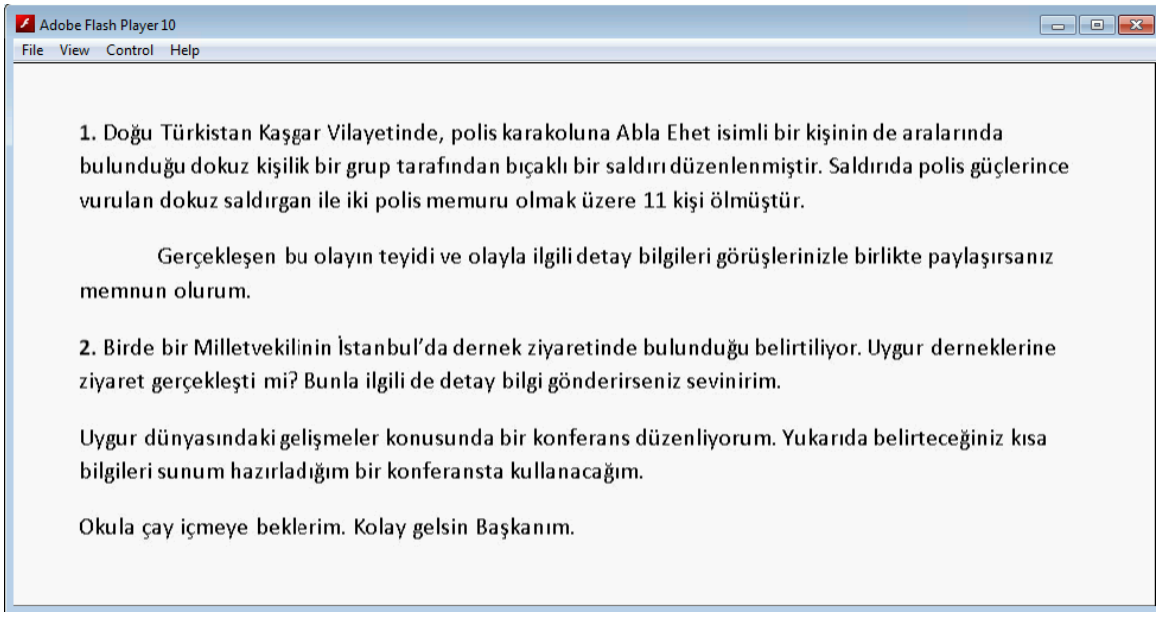
Attack details: Truvasys has been previously documented by peer organizations in the security industry. The malware and its developers have been active for a few years and have conducted multiple attack campaigns by masquerading as common computer utilities such as WinUtils, TrueCrypt, WinRAR, and SanDisk. In each of the campaigns, the Truvasys malware was updated to include additional features, showing close collaboration between the activity groups behind the campaigns and the developers of the malware.

Truvasys is a collection of modules written in the Delphi programming language, a variant of Pascal. It runs on 32-bit and 64-bit editions of multiple versions of Windows, including Windows Vista, Windows 7, Windows 8, and Windows 10, in both standard user and administrator modes. It includes a number of features designed to evade detection, including virtual environment detection and tampering with security software.

Truvasys connects to a remote command and control (C&C) server to retrieve instructions from an attacker, who can use the malware to execute arbitrary functionality on the compromised computer.

This malware family has targeted individuals through the combined use of spear phishing and watering hole techniques for a number of years. In most cases, Truvasys is embedded with legitimate installers of applications, compromising individual computers by tricking users into running the installers. One campaign involved a fake Adobe Flash Player installer, with a social engineering lure in Turkish.

Figure 1. In one campaign, Truvasys was distributed via social engineering lures in the Turkish language



The language used in this example is consistent with the geography of Truvasys victims, as observed over the years. Most Truvasys activities have been observed across western Europe with a large majority of computers using the Turkish locale setting, which suggests that most of them are Turkish citizens or expatriates.

While studying Truvasys, Microsoft uncovered a previously undocumented piece of malware known as Myntor that is a completely separate malware family. Myntor is pushed onto victims' computers that are selected by an unknown logic devised by PROMETHIUM.

Activity Group Profile: NEODYMIUM

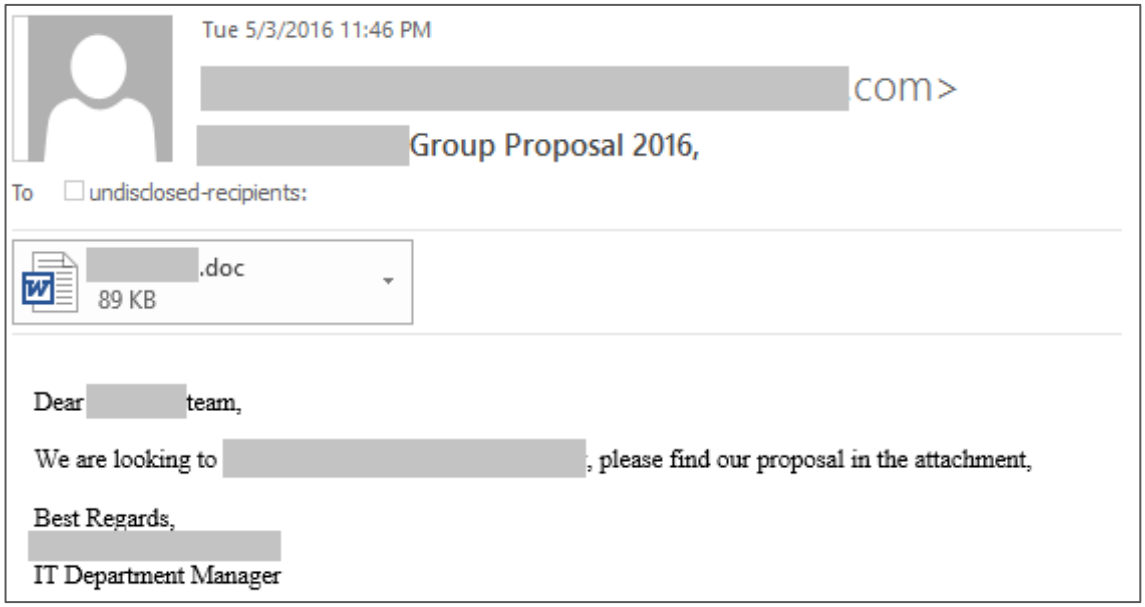
Campaign summary: NEODYMIUM is an activity group that, like PROMETHIUM, conducted an attack campaign in early May 2016. NEODYMIUM also used the exact same CVE-2016-4117 exploit code that PROMETHIUM used, prior to public knowledge of the vulnerability's existence.

NEODYMIUM used a backdoor detected by Windows Defender as Wingbird, whose characteristics closely match FinFisher, a government-grade commercial surveillance package. Data about Wingbird activity indicates that it is typically used to attack individuals and individual computers instead of networks.

Administrators and users wondering whether they were targeted by NEODYMIUM can scan their networks by using the indicators listed in the appendix, by using Windows Defender to examine their logs for "Wingbird," or by searching for NEODYMIUM in their Windows Defender Advanced Threat Protection product console alerts.

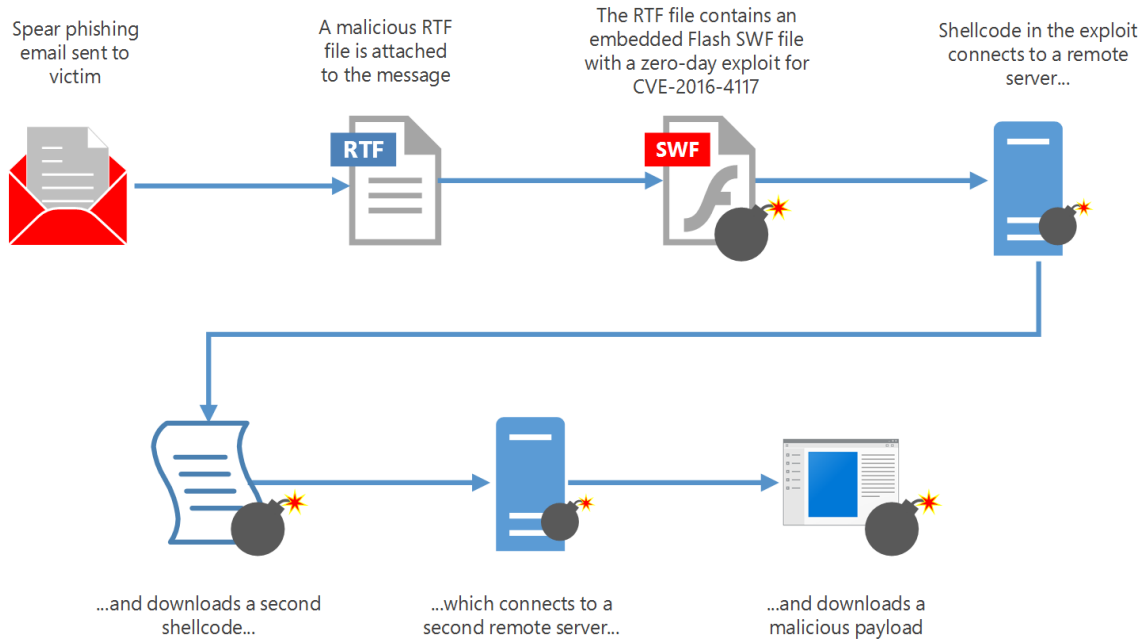
Attack details: Target individuals were sent customized spear phishing emails. An image of one such customized email from this campaign is shown in the following figure.

Figure 2. The spear phishing campaign that NEODYMIUM launched in May 2016 is highly customized to target individuals; a large portion of the email has been redacted to protect the privacy of the targeted individual, which shows the extent of personalization of the malicious email



When the user opened the attachment, a blank document displayed. In the background, a series of events, including the use of the CVE-2016-4117 zero-day exploit, ultimately led to the download and execution of a backdoor. The exploit code executes only if the Microsoft Office Protected View setting is turned off. By default, documents opened from the Internet (using web browsers or email clients) are opened in protected view mode, which prevents execution of embedded objects and potentially malicious code.

Figure 3. The NEODYMIUM attack chain shows how the exploit CVE-2016-4117 was used to infect target individuals' computers



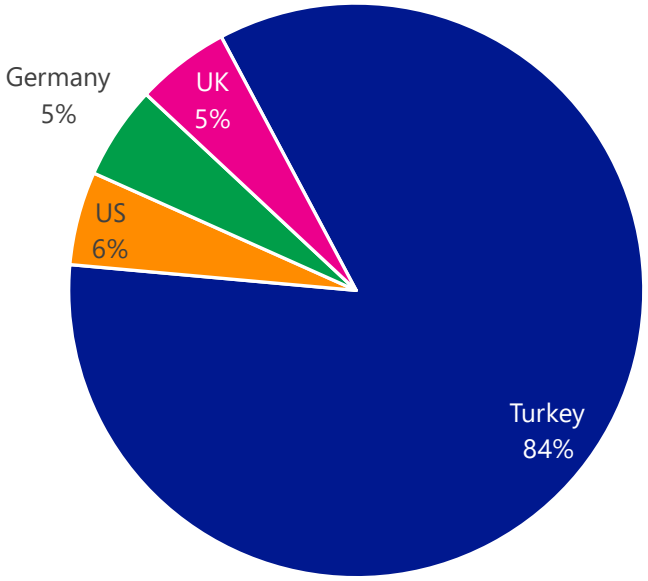
The backdoor payload showed behavior that matched publicly documented traits of a program called FinFisher, a government-grade commercial surveillance package marketed to law enforcement and intelligence agencies. The publisher, FinFisher GmbH, claims that it sells the software exclusively to government agencies for use in targeted and lawful criminal investigations. It is likely that the backdoor payload is a relatively new version of the commercial spyware.

The apparent use of a version of FinFisher suggests that the exploit and the spear fishing campaign that delivered it were the work of an attack group probably connected in some way to a state actor.

Windows Defender detects the backdoor payload as Wingbird. Visibility into the usage of Wingbird shows it has been used only against individuals, not against computers that are part of an organization's network.

Research into Wingbird from May through November 2016 showed only tens of victims, predominantly in Turkey.

Figure 4. NEODYMIUM victim breakdown, by country for May through November 2016

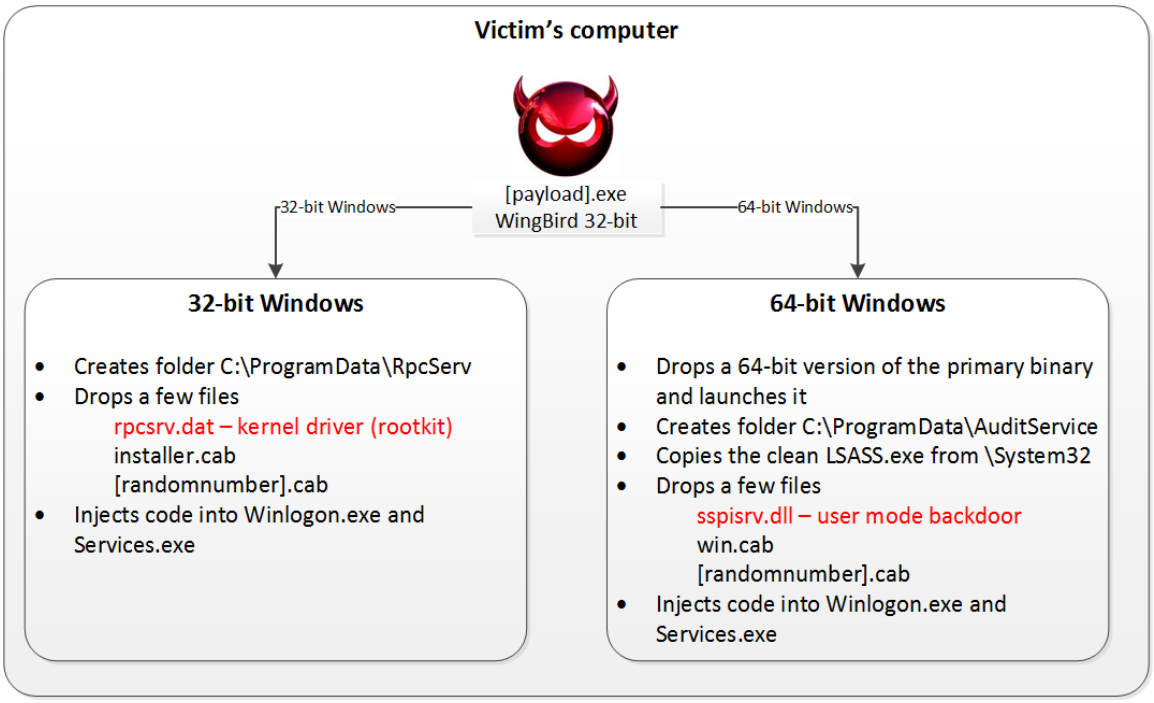


Like Truvasys, Wingbird is designed to run on both 32-bit and 64-bit Windows platforms. The malware is a native 32-bit PE executable that installs a number of additional executables and files. These components are all embedded within the dropper itself, which allows the malware to avoid downloading components and consequently attracting attention.

After the backdoor executes, the malware checks the underlying operating system version and, depending on what platform it is running on, drops several files to %ProgramData%\RpcSrv (on 32-bit computers) or %ProgramData%\AuditService (on 64-bit computers).

In addition, on 64-bit computers the dropper creates a secondary native 64-bit payload executable, referred to in the following diagram as [Payload64].exe. The 32-bit processes are isolated from 64-bit processes and restricted in the actions they can perform. By providing a separate 64-bit payload, Wingbird attempts to inject code into 64-bit processes as well as 32-bit processes.

Figure 5. Wingbird behaves differently on 32-bit computers and 64-bit computers



The main goal of the original dropper is to indirectly deliver executables by injecting malicious code and data into two Windows system processes, Services.exe and Winlogon.exe. The primary Wingbird payload uses anti-VM, anti-debugging, and anti-AV mechanisms to evade discovery and analysis.

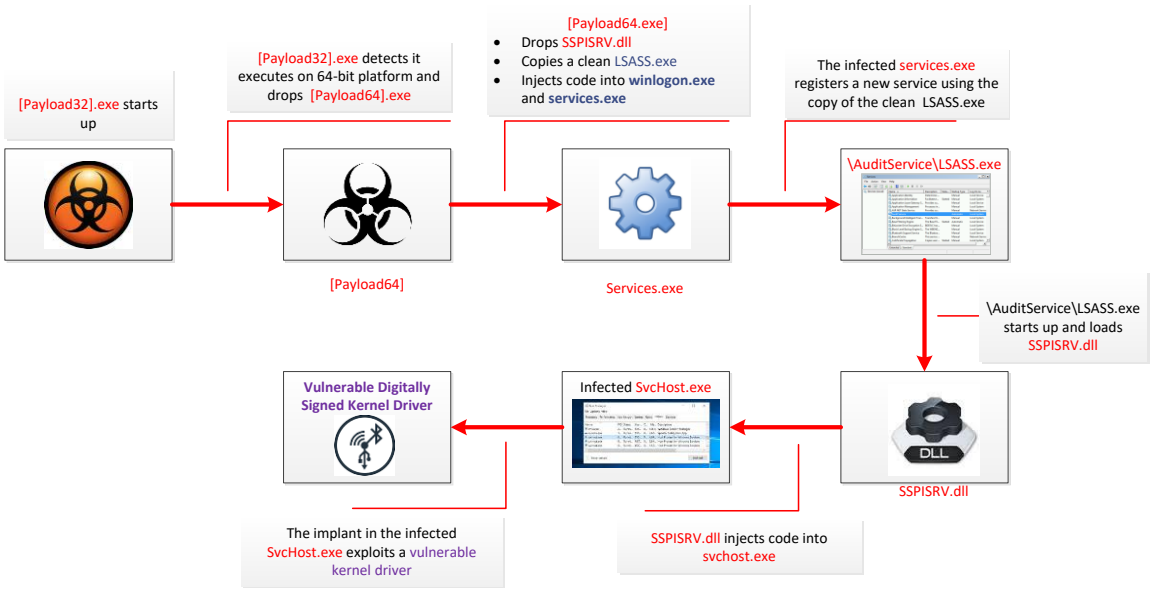
On 32-bit computers, the original dropper creates three files, as shown in Figure 5. Of the three files, the only true binary is rpcsrv.dat, a kernel rootkit that enables the attacker to load and run privileged unsigned code. The other two files, installer.cab and the randomly named [xxxxx].cab, are encrypted data files.

Wingbird attempts to detect and evade security products. For example, some of the strings found in running processes, such as avcuf32.dll and <un-wnd-%.08x>, indicate that the malware checks for the presence of one of several versions of Bitdefender security software.

Through a series of actions and code injections, the original malware installs the rootkit driver, rpcsrv.dat, a non-standard kernel driver. The attackers know that 64-bit computers are much more secure because they prevent loading of unsigned drivers, so they do not even attempt this technique on 64-bit systems. The malware searches for a file called ico_ty23.ico, which is publicly documented as the filename one of the key user mode DLL components of FinFisher.

On 64-bit computers, the installation of Wingbird is a lot more complicated. The 64-bit version of the original payload creates a new folder, %ProgramData%\AuditService, and copies the Windows system file lsass.exe from %SystemFolder% into the new folder. At the same time, the payload drops a malicious file known as sspisrv.dll alongside the copy of lsass.exe. This sspisrv.dll file shares its name with a code library that implements several APIs that lsass.exe is designed to import.

Figure 6. Wingbird payload's behavior on 64-bit computers



The original 32-bit dropper continues monitoring until the folder and file are created. After the 64-bit payload is done copying files, its parent process (the 32-bit dropper) deletes it. The parent process then deletes itself as an attempt to hide its tracks and prevent analysis by security professionals.

The 64-bit malware then injects code into services.exe, the Service Control Manager, to register a service using a clean lsass.exe that would load the malicious sspisrv.dll, which would then inject malicious code into svchost.exe. The constant delegation of malicious code control from one process to the next is a way to hide execution of unwanted code and make it extremely difficult to detect the presence of Wingbird.

This version of Wingbird has also been observed with the ability to execute highly privileged kernel code by injecting code through vulnerable signed

drivers. It maintains a list of legitimate yet vulnerable drivers that can be exploited to inject and execute kernel code.

It appears that Wingbird obfuscates its code at source level, rather than binary level, to evade analysis tools and security solutions.

Similar to the 32-bit version, this version of Wingbird performs a check for a file named ico_sf46.ico, which is a known component of FinFisher.

Mitigation

Stopping zero-day exploits in Windows 10

PROMETHIUM and NEODYMIUM both used a zero-day exploit that executed code to download a malicious payload. Protected view, a security feature that was introduced in Microsoft Office 2010, prevents the malicious Flash code from loading when the document is opened. Control Flow Guard, a security feature that is turned on by default in Windows 10 and Microsoft Office 365 64-bit version, can help by making it more difficult to exploit memory corruption vulnerabilities. The Flash vulnerability CVE-2016-4117 is a type confusion vulnerability in the DeleteRangeTimelineOperation class. The referenced exploit only reliably works on specific Windows platforms because of a ByteArray mitigation in Flash Player, which causes Microsoft to believe that the exploit was authored with pre-knowledge of the victim's computer information. The exploit uses the Adobe Flash Player's Function object vftable corruption method to achieve code execution.

> Control Flow Guard makes it more difficult to exploit memory corruption vulnerabilities.

Because 64-bit versions of Windows 10 enforce driver signing, malicious code that attempts to load a locally made, untrusted driver will be stopped in its tracks.

In addition, the technique of using lsass.exe to load a malicious DLL files can be mitigated by an optional feature introduced in Windows 10 called Credential Guard. Microsoft highly recommends that network administrators test and enable this feature. In Wingbird's case, the malicious sspisrv.dll will not load because it wasn't signed by a trusted certificate.

The Hypervisor Code Integrity (HVCI) service enables the Device Guard feature in Windows 10 to help protect kernel mode processes and drivers from

vulnerability exploits and zero-day exploits. HVCI uses the processor's functionality to force all software running in kernel mode to safely allocate memory, which means that after memory has been allocated, its state must be changed from writable to read-only or execute-only. By forcing memory into these states, HVCI helps ensure that attacks are unable to inject malicious code into kernel mode processes and drivers through techniques such as buffer overflows and heap spraying.

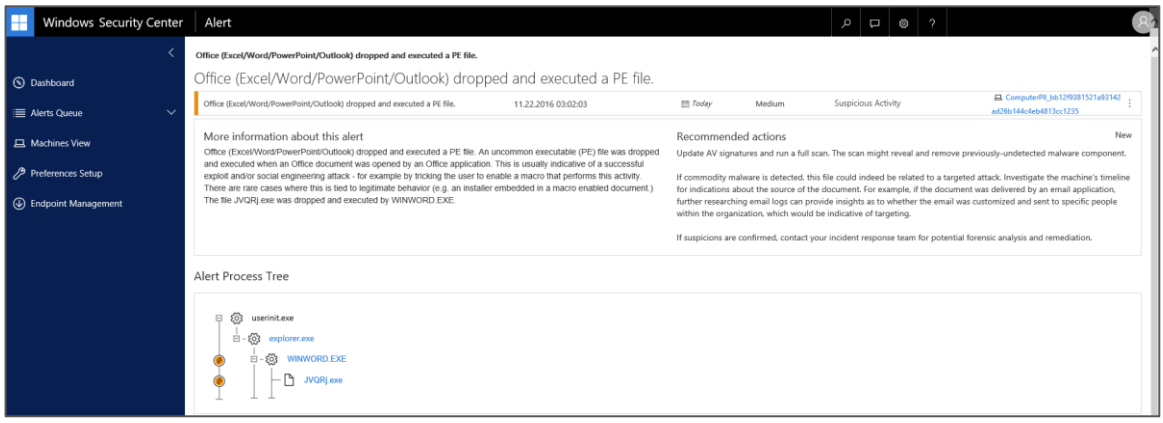
Detecting malicious behavior with Windows Defender Advanced Threat Protection

Windows Defender Advanced Threat Protection (ATP) is a new built-in detection service that ships natively with Windows 10 and helps enterprises to detect targeted and advanced attacks. When activated, it captures behavioral signals from the endpoint and then uses cloud-based security machine learning analytics and threat intelligence to flag suspicious attack-related activities.

The NEODYMIUM attack campaign executed the following five malicious behaviors, all of whichare detected by Windows Defender ATP:

1. Zero-day exploit code causes a Microsoft Office file to generate and open an executable file.

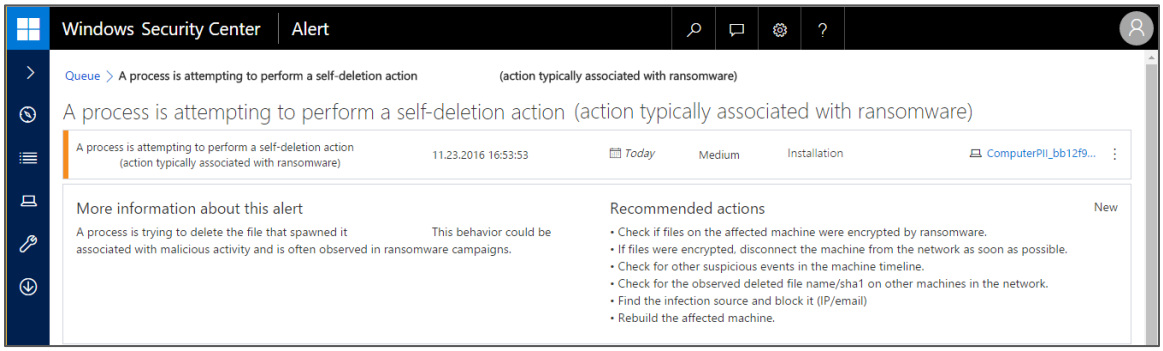
Figure 7. Windows Defender ATP shows an alert for an exploit resulting in a malicious file executing on an endpoint



2. Zero-day exploit code allows an executable file to gain higher privileges.

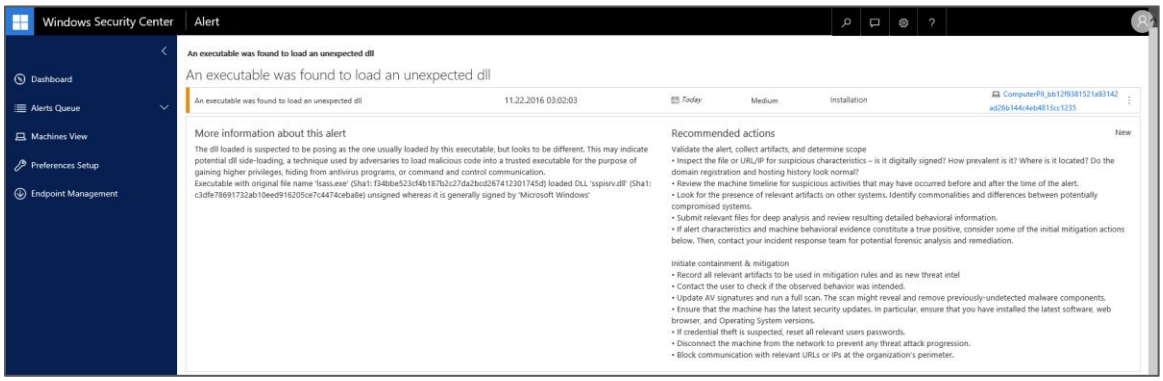
3. A suspicious file self-deletes, a behavior associated with malware that erases traces of infection as a way to evade forensic analysis.

Figure 8. Windows Defender ATP shows an alert for processes that attempt self-deletion



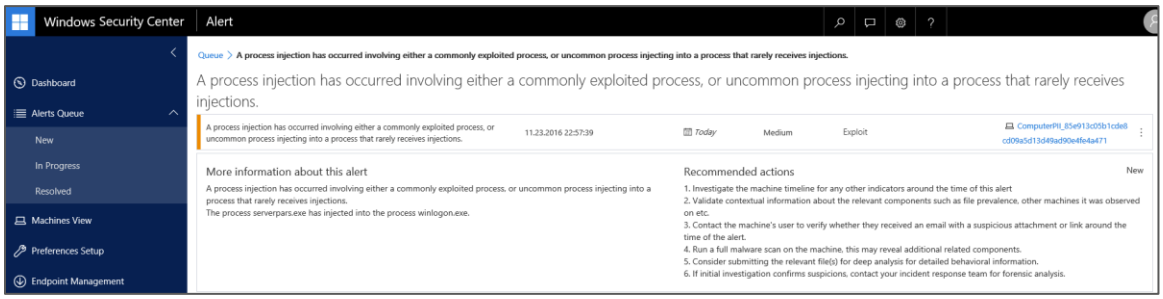
4. Malware executes DLL-side loading, a technique in which attackers replace legitimate DLL files in non-standard folders with malicious ones so that the malicious file is loaded when the application or operating system starts.

Figure 9. Windows Defender ATP shows an alert for DLL-side loading



5. Malware injects code into legitimate processes, which is usually done to load the malware when system processes run.

Figure 10. Windows Defender ATP shows an alert for suspicious code injections



Windows Defender Advanced Threat Protection alerts enterprise security teams of detections and allows them to investigate and respond to each security incident in a timely and effective manner. The service complements and works

along with Windows Defender or third-party antivirus security solutions. Additional information about the service is available here.

Summary

In May 2016, two apparently unrelated activity groups, PROMETHIUM and NEODYMIUM, conducted attack campaigns in Europe that used the same zero-day exploit while the vulnerability was publicly unknown. Although the use of the same exploit code could be attributed to a number of coincidences, the timing of the campaigns and victim demographics lend credence to the theory that the campaigns were associated.

One threat family, Wingbird, appears to be a version of a commercially available tool sold to organizations conducting lawful interception. Wingbird is a fairly advanced threat family that must have required the authors several months' worth of man-hours to generate. Even so, Wingbird as-is does not execute in Windows 10.

Each activity group uses a unique set of tools and methods to perform actions like lateral movement and data exfiltration. One of the purposes of tracking activity groups is to research unique attacker techniques and to develop mitigations for the native operating system. Microsoft has built proactive security mitigations into its products, which increases the investment barrier for attackers who try to victimize users of the latest versions of Windows.

The Windows security service Windows Defender ATP provides an additional post-breach layer of security to enterprises organizations. As this article shows, proactive mitigation in Windows 10 and Office on 64-bit systems does not allow the exploit vector for these two attack campaigns or the exploitation of kernel drivers to succeed. In addition, Windows Defender ATP detects suspicious events on endpoints, alerts security operators about undesired activities, and provides the required tool to respond.

Indicators

The following table includes a sampling of indicators on the malware used by PROMETHIUM and NEODYMIUM. This is just a snippet of the information collected while studying these malware and the corresponding attack campaigns.

Figure 11. PROMETHIUM and NEODYMIUM indicators

SHA1 or other indicator	Association
21a3862dfe21d6b216359c6baa3d3c2beb50c7a3	Malicious document
0b16135d008f6952df0caca104449c33d736e5fc	Malicious document
21a3862dfe21d6b216359c6baa3d3c2beb50c7a3	Malicious document
0852aa6b8df78069d75fa2f09b53d4476cdd252b	Malicious document
05dbe59a7690e28ca295e0f939a0c1213cb42eb0	Wingbird
3c2c7ac8fddbc3ee25ce0f73f01e668855ccdb80	Wingbird
211a111586cb5914876adb929ccae736928d8363	Wingbird
c972bf5751438c99fe3e02ecacf6fa759388c40e	Wingbird
72722073f0adba1919dc31ffa26638555ad5867f	Wingbird
2fb49455d65ad8baf18e3c604cd1b992b7ebbefa	Wingbird
f41b999f41312f2a0fe4eaf08e90824f73e0e186	Wingbird
d8d54574a082162220c3c2f3d3f4c1b1bd4d6255	Wingbird
86580603f5e1d817af87e8bf3ba4dc4ea9e3069d	Wingbird
cb5d0d1d557a1266f77357a951358c78196e97ff	Wingbird
d75d12d250e7a36f9ef1173d630a0059b8ea5349	Wingbird
a77db6e89d604eabf29a6114a30345a705b05107	Wingbird
b32b0d52fff7c09c60bb64bc396dc7522a457399	Wingbird
ade19bde9716770bef84ce4414a45c0462c2eba2	Wingbird
e4d82ab117b86fd44c02ff3289976d15a9d9ced4	Wingbird
88cb78d99fa0275db8123c17a2bd3b3d58f541da	Wingbird
a248f9ad5d757d589a06a253dc46637f4128eea9	Wingbird
532b0d52fff7c09c60bb64bc396dc7522a457399	Wingbird
srv601[.]ddns[.]net	Wingbird
srv602[.]ddns[.]net	Wingbird
980d96d83f0bae8132fd13eb7d0e799999141492	Truvasys
7ab2d32b2603c2b12e814264230572584e157d42	Truvasys
a4f72ee3d337e5a0db78f33fd31958b41e9e9d4f	Truvasys
6de50cf42cd3ff8429a405e9c62d38c11fb2edd6	Truvasys
8d847ea0ffa06b8d48bbd9c943c50b05b23d310b	Truvasys
7047ed9ae510377f4625db256e52af02694ef153	Truvasys
bb66c7d655021234ede01bc59e808c6b8f3fa91b	Truvasys

SHA1 or other indicator	Association
www[.]updatesync[.]com	Truvasys
www[.]svnservices[.]com	Truvasys
ftp[.]mynetenergy[.]com	Truvasys
www[.]windriversupport[.]com	Truvasys
www[.]truecrypte[.]org	Truvasys
www[.]edicupd002[.]com	Truvasys

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