Windows security

Final Project

October 2018

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only, and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third-party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

This training uses various tools and utilities downloaded from the Internet for the classroom environment.   
Downloading any tools, installing and using them should only be done at your own risk security checked the tools in a test environment.

© 2018 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.

Contents

[Windows Security – Final Project 1](#_Toc528227360)

[Abstract 1](#_Toc528227361)

[The Story 1](#_Toc528227362)

[The Mission 1](#_Toc528227363)

[Deliverables 2](#_Toc528227364)

[Evaluation Method 2](#_Toc528227365)

[Annex 1 – Forensic Report 3](#_Toc528227366)

[Fabrikam environment 3](#_Toc528227367)

[General context 3](#_Toc528227368)

[Delivery and installation 3](#_Toc528227369)

[A single ransomware, multiple lateral movement techniques 4](#_Toc528227370)

[Lateral movement using credential theft and impersonation 4](#_Toc528227371)

[Lateral movement using EternalBlue and EternalRomance 6](#_Toc528227372)

[Encryption 7](#_Toc528227373)

[Indicators of Compromise 13](#_Toc528227374)

# Windows Security – Final Project

## Abstract

In this project you will play the role of a Security Consultant hired by the Fabrikam company. Fabrikam was recently the victim of a large-scale ransomware infection. You will enter the game during the remediation phase; forensics investigations have already been conducted. Your role will be to rebuild IT environment which was infected.

## The Story

Fabrikam is one of the largest steel firm in the world. It is a global company, employing nearly 200,000 people worldwide and present in every major economic area. Company’s yearly revenue is around $50 billion.

Two months ago, the company was infected by a variant of the Petya ransomware. This episode literally put the entire IT environment down for 6 weeks. Employee had to bring back pens and papers to run the business. Company factories were forced to close, and furnaces had to be shut down. It takes many weeks to stop or start a furnace. Consequently, production lines were down for a very long time which caused massive losses for the company.

Few days after infection started, Fabrikam commissioned a security company to investigate a couple of machines. The report which was delivered by this company to Fabrikam is available in the Annex section. The report clearly identified IP administration machines as the starting point of the attack.

Like many other companies, Fabrikam IT administrators use to have dedicated workstations to perform administrative tasks like creating accounts in Active Directory or managing the Exchange mail system.

Based on that report, Fabrikam’s IT division decided to rebuild all the admin workstations and deploy a new master designed to meet today’s security best practices.

From organizational point of view, there is a central IT division in charge of providing recommendations, guidance and governance. But each company branch has a forest and its own IT department tasked with administration and security operations. There is no real cooperation between IT departments and the central IT team.

## The Mission

Congratulations! You have been hired as a security consultant by Fabrikam to build this new generation of administration workstations. You will use the recently acquired knowledge about Windows security to propose a new model for Fabrikam’s administration workstations.

## Deliverables

The expected deliverables are:

* A PowerPoint-like presentation. The content of the presentation is generally up to you, but it must include:
  + A risk analysis
  + Clear relation between the risks and associated mitigations
  + Macro planning for the deployment of your solution, including all major phases of the project
* A 12 minutes oral presentation of your proposal

Accepted formats for the presentation are: paper delivery, PowerPoint or PDF.

The presentation will occur on the 15th of November. You can use the presentation to support your talk.

Each group will have exactly 12 minutes to present its work. At the end, you will leave the ppt either printed or file. 12 minutes is a short time period. You are expected to be on time. Any late arrival will be decremented from the 12 minutes.

Presentation will be performed in French.

There will be 1 Q&A exchange with the customer. The process to ask questions is:

1. Formalize the list of questions you have for the customer in an Excel, Word or text document
2. Send it to the customer before November 5th at 23:55
3. Customer will answer questions starting on November 6th

Q&A constraints:

* You can upload as many questions lists as you want but customer will only read the last uploaded document
* Customer won’t answer any question sent after November 6th

## Evaluation Method

This paragraph explains how your work is going to be evaluated during the presentation session.

At all time, keep in mind that the goal of the project is to train yourself into real-life delivery of a security project. It particularly means that you must not underestimate the non-technical aspects of the project.

Important criteria which will define the success or failure of your performance:

* Ability to demonstrate relevance of any technical product or functionality. Security costs money and the organization won’t spend money in a solution if it does not see its value.
* Ability to demonstrate knowledge of security threats, products or features by being able to explain it in a concise and simple way to a non-expert public (CIO, CISO, …) in a very short amount of time
* Ability to understand the complexity of solutions by being able to determine a reasonable amount of effort to deploy proposed technology
* Presentation skills

## Annex 1 – Forensic Report

#### Fabrikam environment

Fabrikam’s IT environment is composed of 35 Active Directory forests, 8000 servers and 100000 workstations and laptops.

Fabrikam has various operating systems from Windows XP/2003 to Windows Server 2016/Windows 10 RS2. A forest is dedicated to host Exchange 2016 for all the company. Branches also relies on other environments like SAP, factory industrial computers (Linux, Windows CE, MSDOS 3.11, and more).

#### General context

On June 27, 2017 reports of a [ransomware](https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx) infection began spreading across Europe. We saw the first infections in Ukraine, where more than 12,500 machines encountered the threat. We then observed infections in another 64 countries, including Belgium, Brazil, Germany, Russia, and the United States.

The new ransomware has worm capabilities, which allows it to move laterally across infected networks. Based on our investigation, this new ransomware shares similar codes and is a new variant of [Ransom:Win32/Petya](https://www.microsoft.com/en-us/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/Petya). This new strain of ransomware, however, is more sophisticated.

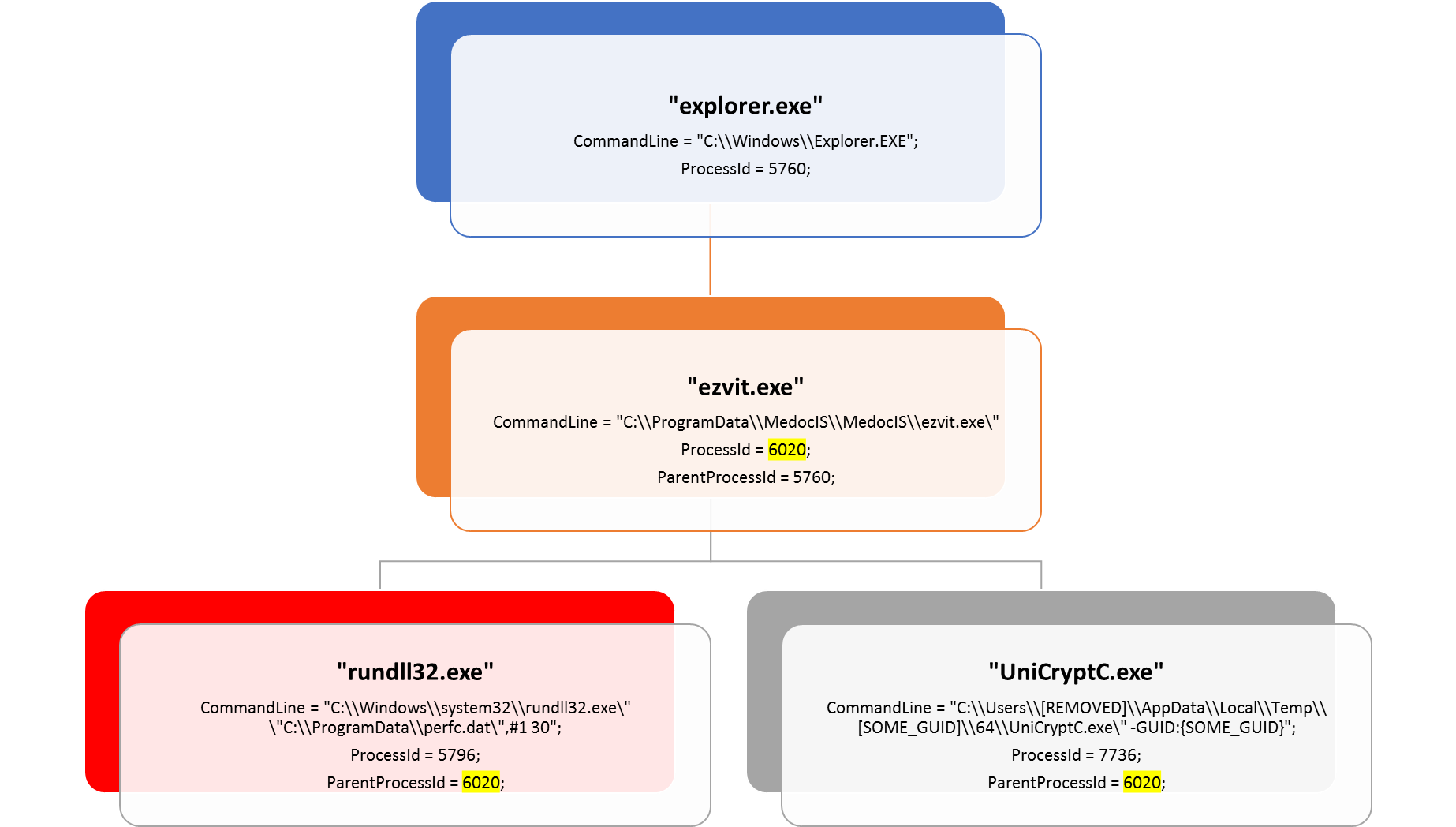
#### Delivery and installation

Initial infection appears to involve a software supply-chain threat impacting the administration tools of the accounting software application MEDoc. We now have evidence that a infections of the ransomware initially started from the legitimate MEDoc updater process. As we highlighted on our blog, [software supply chain attacks](https://blogs.technet.microsoft.com/mmpc/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-supply-chain-cyberattack/) are a recent dangerous trend with attackers, and it requires advanced defense.

According to our investigations, we observed the MEDoc software updater process (*EzVit.exe)* executing a malicious command-line matching this exact attack pattern on Tuesday, June 27 around 10:30 a.m. GMT.

The execution chain leading to the ransomware installation is represented in the diagram below and essentially confirms that*EzVit.exe* process from MEDoc, for unknown reasons, at some moment executed the following command-line:

*C:\\Windows\\system32\\rundll32.exe\” \”C:\\ProgramData\\perfc.dat\”,#1 30*



#### A single ransomware, multiple lateral movement techniques

Given this ransomware’s added lateral movement capabilities it only takes a single infected machine to affect a network. The ransomware spreading functionality is composed of multiple methods responsible for:

* + stealing credentials or re-using existing active sessions
  + using file-shares to transfer the malicious file across machines on the same network
  + using existing legitimate functionalities to execute the payload or abusing SMB vulnerabilities for unpatched machines

In the next sections, we discuss the details of each technique.

#### Lateral movement using credential theft and impersonation

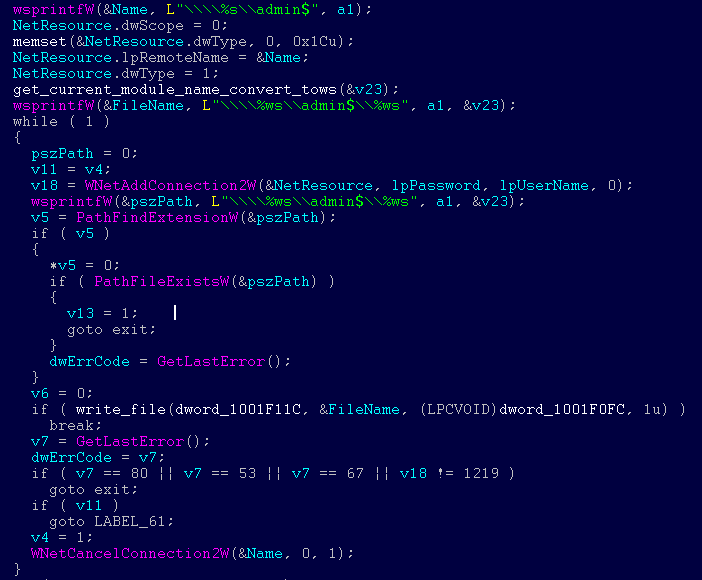
This ransomware drops a credential dumping tool (typically as a .tmp file in the *%Temp%* folder) that shares code similarities with [Mimikatz](https://www.microsoft.com/en-us/security/portal/threat/encyclopedia/Entry.aspx?Name=HackTool:Win32/Mimikatz) and comes in 32-bit and 64-bit variants. Because users frequently log in using accounts with local admin privileges and have active sessions opens across multiple machines, stolen credentials are likely to provide the same level of access the user has on other machines.

Once the ransomware has valid credentials, it scans the local network to establish valid connections on ports *tcp/139* and *tcp/445*. A special behavior is reserved for Domain Controllers or servers: this ransomware attempts to call *DhcpEnumSubnets()* to enumerate DHCP subnets; for each subnet, it gathers all hosts/clients (using *DhcpEnumSubnetClients()*) for scanning for *tcp/139* and *tcp/445* services. If it gets a response, the malware attempts to copy a binary on the remote machine using regular file-transfer functionalities with the stolen credentials.

It then tries to execute remotely the malware using either PSEXEC or WMIC tools.

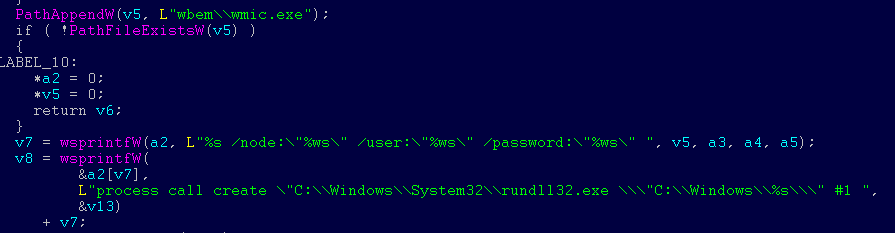
The ransomware attempts to drop the legitimate *psexec.exe* (typically renamed to *dllhost.dat*) from an embedded resource within the malware. It then scans the local network for *admin$* shares, copies itself across the network, and executes the newly copied malware binary remotely using PSEXEC.

In addition to credential dumping, the malware also tries to steal credentials by using the *CredEnumerateW* function to get all the other user credentials potentially stored on the credential store. If a credential name starts with *“TERMSRV/”* and the type is set as 1 (generic) it uses that credential to propagate through the network.



*Ransomware code responsible for accessing* [*\\Admin$*](file:///\\Admin$) *shares on different machines*

This ransomware also uses the Windows Management Instrumentation Command-line (WMIC) to find remote shares (using *NetEnum/NetAdd*) to spread to. It uses either a duplicate token of the current user (for existing connections), or a username/password combination (spreading through legit tools).

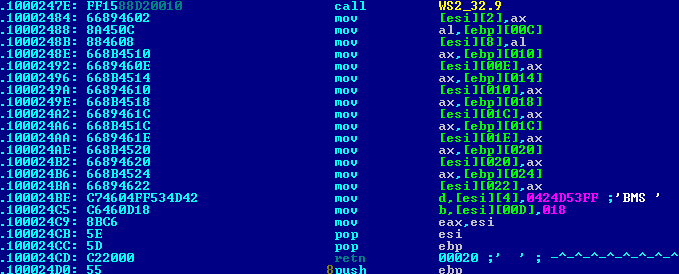


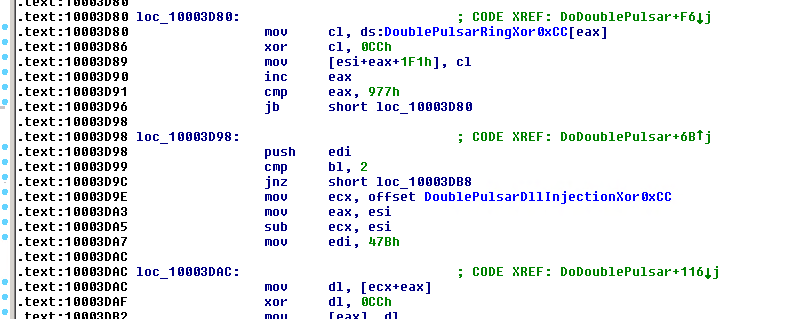
*Screenshot showing launch of malware on a remote machine using WMIC*

#### Lateral movement using EternalBlue and EternalRomance

The ransomware can also spread using an exploit for the Server Message Block (SMB) vulnerability [CVE-2017-0144](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144) (also known as EternalBlue), which was fixed in [security update MS17-010](https://technet.microsoft.com/en-us/library/security/ms17-010.aspx) and was also exploited by [WannaCrypt](https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/) to spread to out-of-date machines. In addition, this ransomware also uses a second exploit for [CVE-2017-0145](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145) (also known as EternalRomance, and fixed by the same bulletin).

We’ve seen this ransomware attempt to use these exploits by generating SMBv1 packets (which are all *XOR 0xCC* encrypted) to trigger these vulnerabilities at the following address of the malware code:



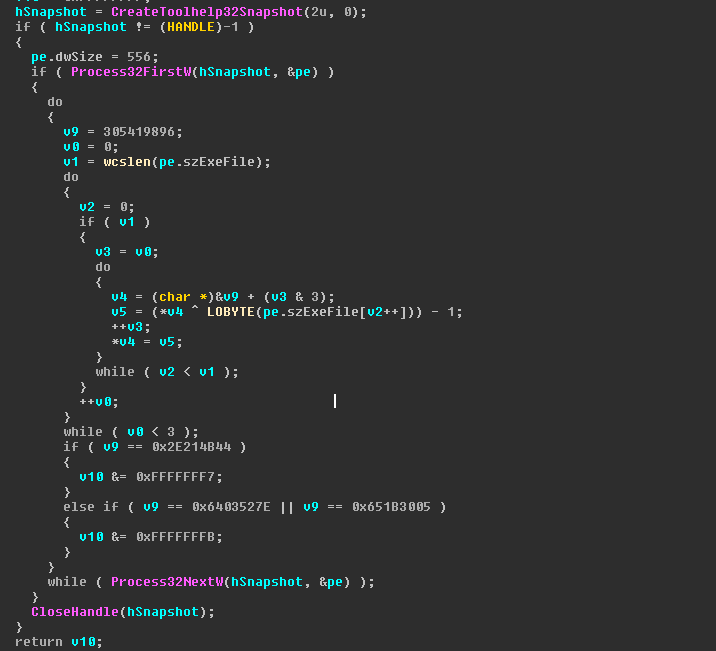


These two exploits were leaked by a group called [Shadow Brokers](https://blogs.technet.microsoft.com/mmpc/2017/06/16/analysis-of-the-shadow-brokers-release-and-mitigation-with-windows-10-virtualization-based-security/). However, it is important to note that both of these vulnerabilities have been fixed by Microsoft in [security update MS17-010](https://technet.microsoft.com/en-us/library/security/ms17-010.aspx) on March 14, 2017.

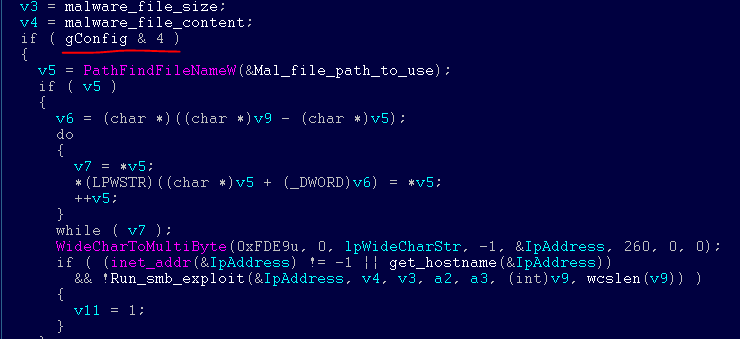
Machines that are patched against these exploits (with [security update MS17-010](https://technet.microsoft.com/en-us/library/security/ms17-010.aspx)) or [have disabled SMBv1](https://support.microsoft.com/kb/2696547) are not affected by this particular spreading mechanism. Please refer to our previous [blog](https://blogs.technet.microsoft.com/mmpc/2017/06/16/analysis-of-the-shadow-brokers-release-and-mitigation-with-windows-10-virtualization-based-security/) for details on these exploits.

#### Encryption

This ransomware’s encryption behavior depends on the malware process privilege level and the processes found to be running on the machine. It does this by employing a simple XOR-based hashing algorithm on the process names, and checks against the following hash values to use as a behavior exclusion:



* + *0x6403527E* or *0x651B3005* – if these hashes of process names are found running on the machine, then the ransomware does not do SMB exploitation.



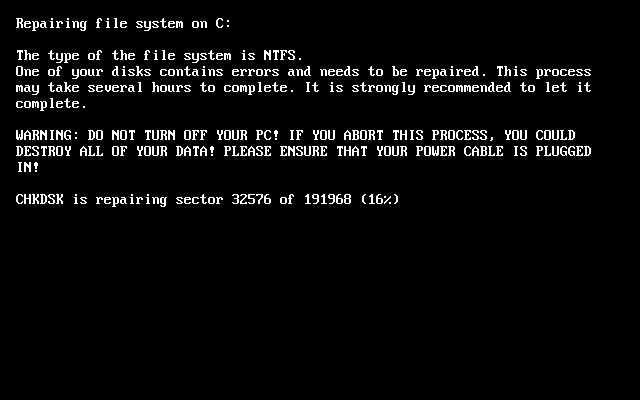
* + *0x2E214B44*– if a process with this hashed name is found, the ransomware trashes the first 10 sectors of [*\\\\.\\PhysicalDrive0*](file:///\\PhysicalDrive0), including the MBR.

C:\Users\bboucken\AppData\Local\Temp\msohtmlclip1\02\clip_image009.png

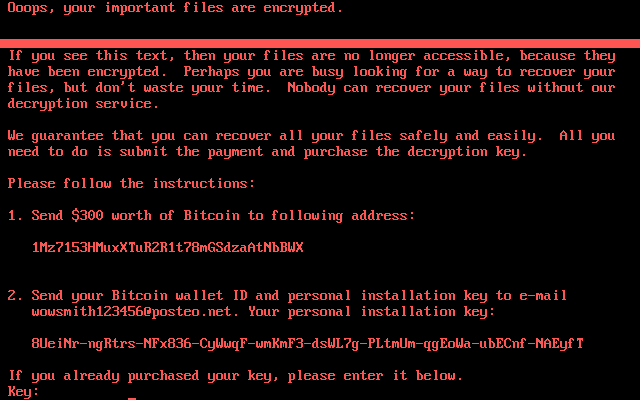
This ransomware then writes to the master boot record (MBR) and then sets up the system to reboot. It sets up scheduled tasks to shut down the machine after at least 10 minutes past the current time. The exact time is random *(GetTickCount())*. For example:

*schtasks /Create /SC once /TN “” /TR “<system folder>\shutdown.exe /r /f” /ST 14:23*

After successfully modifying the MBR, it displays the following fake system message, which notes a supposed error in the drive and shows the fake integrity checking:



It then displays this ransom note:

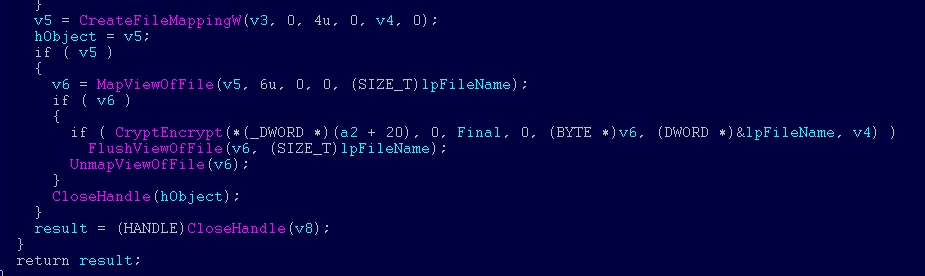


Only if the malware is running with highest privilege (i.e., with *SeDebugPrivilege* enabled), it tries to overwrite the MBR code.

This ransomware attempts to encrypt all files with the following file name extensions in all folders in all fixed drives, except for *C:\Windows*:

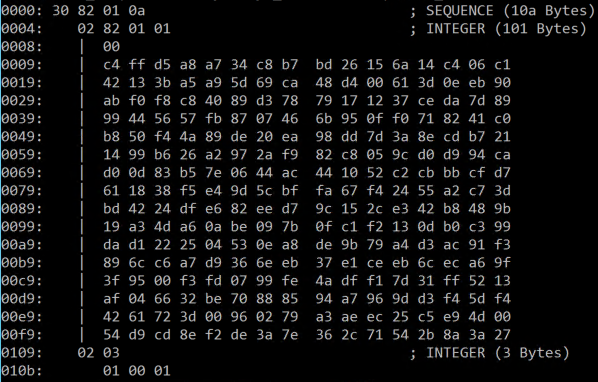
|  |  |  |  |
| --- | --- | --- | --- |
| .3ds | .7z | .accdb | .ai |
| .asp | .aspx | .avhd | .back |
| .bak | .c | .cfg | .conf |
| .cpp | .cs | .ctl | .dbf |
| .disk | .djvu | .doc | .docx |
| .dwg | .eml | .fdb | .gz |
| .h | .hdd | .kdbx | .mail |
| .mdb | .msg | .nrg | .ora |
| .ost | .ova | .ovf | .pdf |
| .php | .pmf | .ppt | .pptx |
| .pst | .pvi | .py | .pyc |
| .rar | .rtf | .sln | .sql |
| .tar | .vbox | .vbs | .vcb |
| .vdi | .vfd | .vmc | .vmdk |
| .vmsd | .vmx | .vsdx | .vsv |
| .work | .xls | .xlsx | .xvd |
| .zip |  |  |  |
|  |  |  |  |

It uses file mapping APIs instead of a usual *ReadFile()*/*WriteFile()* APIs:

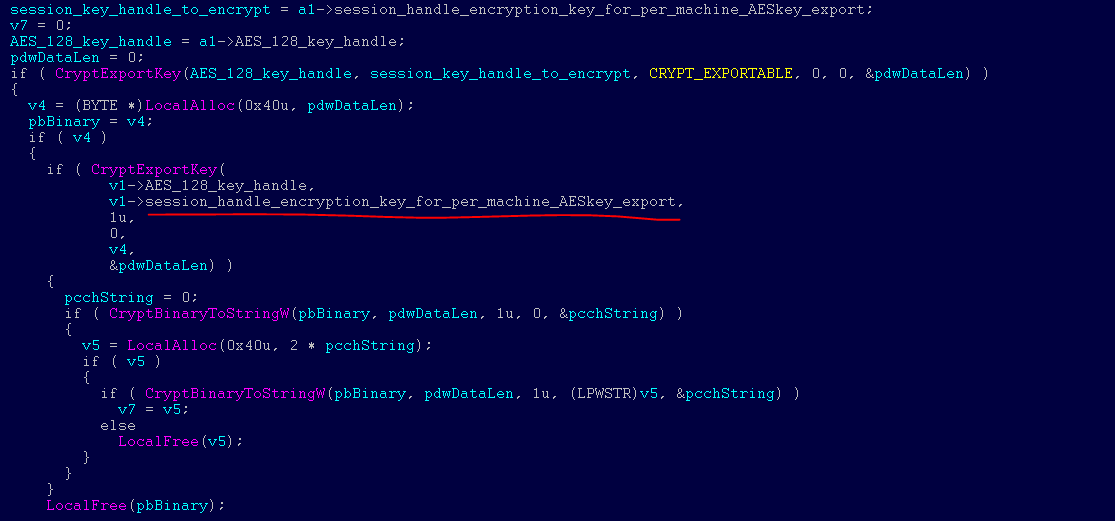


Unlike most other ransomware, this threat does not append a new file name extension to encrypted files. Instead, it overwrites the said files.

The AES key generated for encryption is per machine, per fixed drive, and gets exported and encrypted using the embedded 2048-bit RSA public key of the attacker.



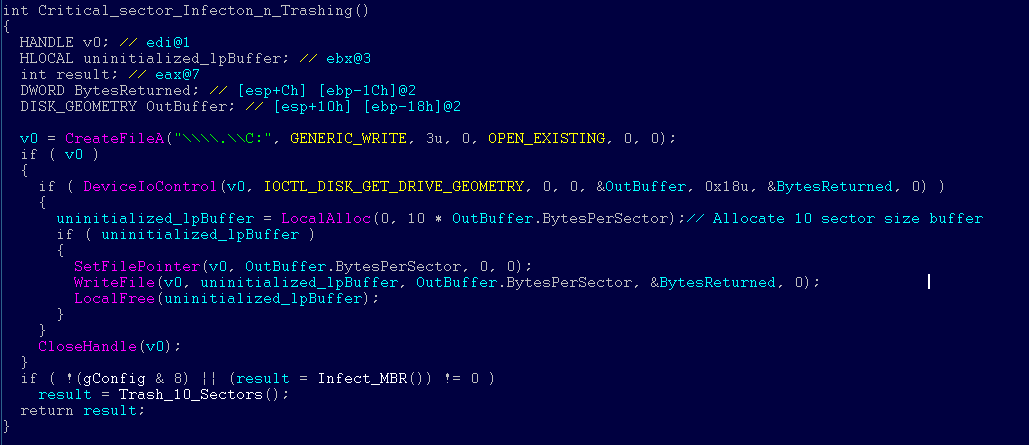
*Embedded RSA public key*



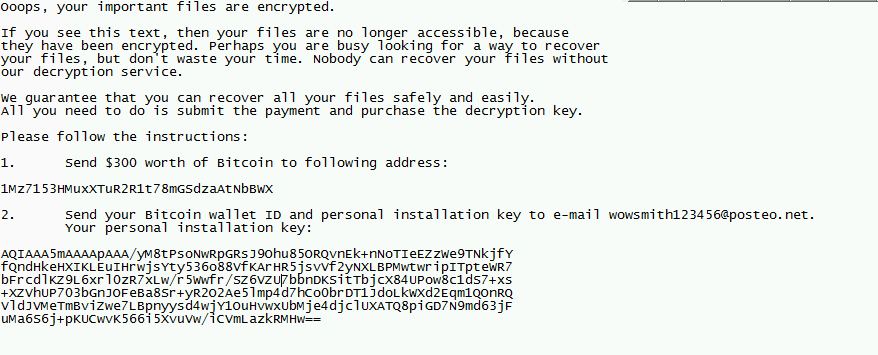
*Code exporting the AES 128 bit key per machine, per fixed drive in the machine and encrypting it using embedded RSA public key during export*

The unique key used for files encryption (AES) is added, in encrypted form, to the *README.TXT* file the threat writes under section *“Your personal installation key:”*.

Beyond encrypting files, this ransomware also attempts to infect the MBR or destroy certain sectors of VBR and MBR:



After completing its encryption routine, this ransomware drops a text file called *README.TXT* in each fixed drive. The said file has the following text:



This ransomware also clears the System, Setup, Security, Application event logs and deletes NTFS journal info.

#### Indicators of Compromise

Network defenders may search for the following indicators:

###### File indicators

* + 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
  + 9717cfdc2d023812dbc84a941674eb23a2a8ef06
  + 38e2855e11e353cedf9a8a4f2f2747f1c5c07fcf
  + 56c03d8e43f50568741704aee482704a4f5005ad

###### Command lines

In environments where command-line logging is available, the following command lines may be searched:

* + Scheduled Reboot Task: Petya schedules a reboot for a random time between 10 and 60 minutes from the current time
  + *schtasks /Create /SC once /TN “” /TR “<system folder>\shutdown.exe /r /f” /ST <time>*
  + *cmd.exe /c schtasks /RU “SYSTEM” /Create /SC once /TN “” /TR “C:\Windows\system32\shutdown.exe /r /f” /ST <time>*

This may be surfaced by searching for EventId 106 (General Task Registration) which captures tasks registered with the Task Scheduler service.

* + Lateral Movement (Remote WMI)
  + *“process call create \”C:\\Windows\\System32\\rundll32.exe \\\”C:\\Windows\\perfc.dat\\\” #1″*

###### Network indicators

In environments where NetFlow data are available, this ransomware’s subnet-scanning behavior may be observed by looking for the following:

* + Workstations scanning ports tcp/139 and tcp/445 on their own local (/24) network scope.
  + Servers (in particular, domain controllers) scanning ports tcp/139 and tcp/445 across multiple /24 scopes.