

Cyber Threat Intelligence: Analysis of Ransomware

Mohammad bin Omar Jawaid

Science, Engineering & Environment, University of Salford

CTI (LS-11) Cyber Threat Intelligence

Dr. Lee Speakman

March 18, 2025

Abstract

In 2017 WannaCry ransomware attack was a global cyber incident which exploited the EternalBlue vulnerability (CVE-2017-0144) to rapidly impact on unpatched Windows systems. This report describes a WannaCry attack as a cybersecurity incident using the Cyber Threat Intelligence (CTI) framework and its Threat Intelligence Cycle to explore attack vectors, the motives of an adversary, impact and mitigation strategies. This attack severely found the healthcare, finance and its government greatly affected; with the National Health Services (NHS) lost by the UK about £ 92 million.

WannaCry's self propagation, encryption mechanisms and Indicators of Compromise (IoCs) were found through intelligence collection. Attack also showed weakness in patch management, sharing real time threat intelligence making it easier for virus writers to target the computer with malicious software, and also showed weakness in incident response coordination. Ransomware is still growing and evolving as Ransomware as a Service (RaaS) and double extortion tactics.

This report also implies such measures as automated patch deployment, segregation of the network, advanced endpoint detection, and proactive intelligence and sharing of threats. However, challenges persist in realms of real time intelligence collaboration, as well as in the latest tactics of today's ransomware. Future examinations should concentrate on AI beneficial threat discovery, blockchain based on backup answers, and worldwide security strategy to hold up against ransomware dangers.

Keyword: WannaCry, Ransomware, CTI, EternalBlue, RaaS, NHS, Blockchain Backup Solutions, Healthcare, Attack Vectors

Table of Contents

Abstract	2
Introduction	4
Overview	4
Main Body – Cyber Threat Intelligence Analysis	7
Application of the Threat Intelligence Cycle	8
Malware Analysis	10
Dynamic Analysis Report	16
Conclusion	24
Recommendations	25
References	25

Introduction

Ransomware is among the most common and damaging forms of malware, which encrypts the victims' data and then demands payment in order to release them. Ransomware attacks have escalated both in number and severity over the last decade and have damaged organizations across all major industry sectors, such as healthcare. These attacks have resulted in financial and operational disruptions strongly urging for robust security measures.

Organizations can build a stronger defensive strategy by gathering intelligence on how cyber criminals use tactics, techniques and procedures, or TTPs. An intelligence driven approach to cybersecurity allows enterprises to not only predict threats, elevate incident response capabilities but also reduce ransomware attacks. The report by ENISA Threat Landscape 2024 confirms a trend of increasing sophistication of cyber criminals who are maltreating information security with threat intelligence at the core of modern information security framework (ENISA, 2024).

Based on the cyber threat intelligence cycle, this report intends to give a detailed analysis on ransomware as a major cyber threat. This report has the following objectives:

- To examine the evolving ransomware threat landscape, including motivations, attack vectors, and key adversary profiles.
- To analyze a recent ransomware intrusion campaign, highlighting the methodologies used by attackers and the impact on targeted organizations.
- To assess the challenges of threat intelligence in combating ransomware, identifying gaps in existing security measures.
- To propose intelligent and cost-effective mitigation strategies based on industry

Rosenstein, R. (n.d.). quotes "Whether you work for local law enforcement, a utility provider, a hospital, or a small or large company, you need to protect your critical infrastructure against cyber infiltration. The threat that cybercriminals pose to public entities and private businesses is substantial. A single intrusion could mean economic loss, bankruptcy, and in some cases, loss of human life."

Overview

Background Information

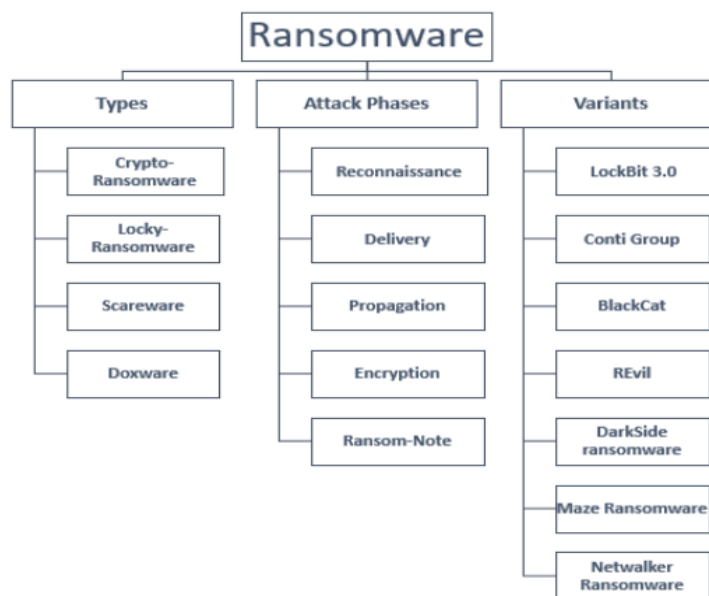
Ransomware is one of the major cybersecurity threats in place that poses a high level of disruption and financial cost to several industries. Malicious software of this type enforces encryption of critical data or systems that are held inaccessible until ransom is paid. "In the majority of cases, ransomware attacks are motivated by financial gain. Cybercriminals deploy ransomware with the primary objective of extorting monetary compensation from their victims" (Temara, 2024, p.6). The main concern is ransomware attacks across all of the sectors, healthcare, government, and finance, which causes their operational shutdowns, data breaches, and even damages their reputation. Ransomware is an increasing problem in healthcare, threatening patients' lives by ruining vital services and theft of patient records.

Table 1 Descriptive statistics of victim companies of different sectors. Mean and median revenue are in million euros, insured, no backup, and paid are percentages. Financial loss and ransom are in thousand euros (Meurs et al., 2022).

	Sector	Number of attacks	Mean Revenue (Meuro)	Median Revenue (Meuro)	(%) Insured	(%) No Backup	Financial Loss (euro)	(%) Ransom Paid	Ransom Requested (euro)
1	Construction	53	562.84	2.43	10.2	35.3	256,410	27.5	182,840
2	Healthcare	21	37.62	2.33	10.5	42.9	77,690	26.3	23,770
3	Trade	113	133.96	2.84	4.9	38.9	737,610	25.5	1,106,800
4	ICT	60	120.59	3.81	13	30.8	232,580	30.9	1,343,190
5	MAS	12	376.36	0.63	0	18.2	12,500	9.1	13,700
6	Media	20	142.54	3.30	0	52.9	344,800	15.8	11,640
7	Education	14	101.43	19.44	0	14.3	49,800	21.4	555,660
8	Government	10	60.17	18.45	10	20	393,330	0	820,350
9	Leisure	20	6.61	1.08	15	55	27,000	15	81,020
10	Transport	29	389.05	6.00	7.4	34.6	838,85	30.8	529,540

From figure 1, we could see the stages of a ransomware attack that normally follow a predictable pattern. Once attackers are aware of what is out there, reconnaissance is done with OpenSource Intelligence (OSINT) to find weaknesses. Then, along with poor credentials or phishing emails, the ransomware is delivered to propagate laterally throughout networks. With strong encryption algorithms, attackers encrypt the victim's data and it becomes impossible to recover without a decryption key. A ransom note is finally issued, widening the public demand to pay—from via cryptocurrency—to either restore data or to prevent its public release.

Figure 1 Ransomware study taxonomy (Adapted from Prasad and Kumar, 2024, p. 1).



Ransom payments get only a small share of a ransomware's actual toll on organizations: downtime, regulatory penalties, and reputational damage. Remediation costs for high profile cases, such as 2017 NHS ransomware attack, are almost always more than the ransom. Ransomware attacks in healthcare not only disrupt the operations, but the patients' privacy is also compromised. (Srivastava, Faist, Lickert, Neville, McCarthy, Fehling-Kaschek, & Stolz, 2024, p. 1) states that the 2016 Lukaskrankenhaus Neuss attack that caused a five day outage on the system [as well as the 2021 Conti ransomware attack against Ireland's Healthcare Services Executive, which resulted in patient care being impacted].

Literature Review

Ransomware is becoming the new cybersecurity threat and the attacks are becoming more frequented and sophisticated. The WannaCry ransomware attack of 2017 showed how devastating ransomware could be in healthcare, government and financial center industries with the EternalBlue vulnerability (CVE-2017-0144) being exploited to spread over unpatched networks (Trautman & Ormerod, 2019). Ransomware attacks follow a process of planned stages from reconnaissance and infection to encryption and ransom demands (Prasad & Kumar, 2024). Phishing is the main social engineering technique used by attackers to infiltrate networks (Gallegos-Segovia et al., 2017).

There is currently research on how ransomware has been evolving and ways to overcome it. The creation of Ransomware as a Service (RaaS), cybercrime has no need of technical expertise whatsoever to carry out large scale attacks (Chesti et al., 2020). Early detection techniques such as identifying ransomware patterns using machine learning are presented as highlighted in the studies (Albshaier et al., 2024). Besides, cyber threat intelligence too serves the purpose of finding the Indicators of compromise (IoCs) and devising proactive mitigation strategies (ENISA, 2024).

Continuing as a prime target, the 2021 Conti ransomware attack against Ireland's Healthcare Services Executive is an example of this (Srivastava et al., 2024). Still in the news, ancient scribes and researchers believe we should implement more cyber security policies, use AI to alert failed detective systems and devise reliable backups regarding ransomware risks (Ansori et al., 2024). Even now, despite advancements, the threat of ransomware is advancing as well and we need to continue to research new ways to defend ourselves against it (Benmalek, 2024).

Scope

The objective of this research is to analyze the effect of ransomware attacks on hospital systems specifically, in terms of its impact on patient care, data security and continuity of the operations. It will take a look at attack vectors, ransomware deployment technical mechanisms, and the havoc these wreak with the hospital infrastructure. It will also study the monetary impacts of the ransomware attack, including financial fees and expenses due to recovery, as well as the mental impacts on hospital staff and patients.

Limitations

This research faces several limitations, including access to other attacks' detailed information about specific ransomware attacks used in this research is restricted since they are confidential. As we know, the nature of ransomware evolves very quickly, so future ransomware can bring us new challenges that may not be provided by this analysis. The main theme of the study will be on the direct impact of ransomware on hospitals systems, rather on the systemically wide preparation that affects the health sector. Moreover, the findings may be applicable to all hospital settings only partially, given variations.

Main Body – Cyber Threat Intelligence Analysis

Overview of the Selected Cyber Threat

Description of the Recent Intrusion Campaign – WannaCry 2017

In May 2017, WannaCry ransomware attack was a global cyberattack which targeted computers running Microsoft Windows. Files were then encrypted and money was demanded in Bitcoin. WannaCry utilized an exploit known as EternalBlue, which was developed by NSA, and leaked by a hacking group called The Shadow Brokers. From table 2, we could see main features and impact of ransomware.

Microsoft had already released security patches, which were used before the attack, but the patching was not widespread enough in many organizations leaving them vulnerable. WannaCry infected over 300,000 computers in 150 countries which caused financial losses in the billions of dollars. Modern ransomware has evolved into a highly sophisticated and organized cyber threat, with variants such as WannaCry, Petya, and CryptoLocker causing substantial financial losses globally. These attacks not only impact individuals but also target large organizations and critical infrastructure, emphasizing the severity of the threat and the need for strong mitigation strategies and defense mechanisms (Ansori et al., 2024, p. 1).

Table 2 Main Feature and Impact of WannaCry adapted from (Albshaier, Almarri, & Rahman, 2024, p. 10)

Year	Notable Ransomware	Main Features	Impact
2017	WannaCry, Bad Rabbit	Exploited EternalBlue vulnerability	Caused global panic due to rapid spread through networks by exploiting unpatched Windows Server Message Block (SMB) protocol vulnerabilities—SMB is a network protocol used for file sharing; prompted urgent global security updates.

The kill switch domain in the code of the ransomware was found by Marcus Hutchins, a cybersecurity researcher, before the ransomware could spread further.

The UK's National Health Service (NHS) was one of the most heavily affected organizations. Hospitals were badly hit with major disruption that saw cancelled surgeries, delayed treatments and emergency service failures. Financial losses of about £92m were also suffered by the NHS from IT upgrades and operational disruption (Avast, n.d.).

Adversaries Involved, Their Motives, and Attack Techniques

Primary Suspect: (Trautman & Ormerod, 2019, p. 23) suspects that the United States and the United Kingdom attributed the attack to North Korea, though North Korea denied any involvement.

Motive: WannaCry is believed to have been used for financial gain, as ransom payments were demanded in Bitcoin. Some theories also suggest state-sponsored cyber warfare.

Attack Techniques:

Propagation Mechanism: WannaCry is a ransomware cryptoworm, meaning it self-propagates across networks without user interaction.

Exploits Used: An exploit of the Server Message Block (SMB) protocol, allowing attackers to gain unauthorized access to unpatched systems. (Wikipedia contributors, n.d., "Propagation Mechanism and Exploits Used" section)

Application of the Threat Intelligence Cycle

Planning and Direction

When Intelligence Requirements (IRs) to review and counteract WannaCry attacks are determined. It confirms coordinated efforts toward intelligence and increases efficiency of the resources used. Amongst the packing actions are shaping objectives like understanding how WannaCry used the EternalBlue vulnerability, identification of secured frameworks, characterization of its encryption procedures and exploration of the execution of Kill Switch. Heavily impacted organizations such as UK's National Health Service, examine the timeline of the attack, and determine whether the unpatched systems are a consequence of MS17-010 release. A collection plan consists of gathering malware samples, network logs, ransom notes. Different teams will be given different security resources, such as SOC teams for monitoring, threat intelligence analysts for the data gathering, incident responders for tracking the ransom payments.

Collection

Collecting raw data from various sources to understand the WannaCry attack. Identifying relevant data sources, such as the malware samples that security researchers have collected, as well as Microsoft and Symantec reports is among key action groups. For tasking, one needs to examine vulnerable Windows systems and track ransom transactions. SMB activity is monitored, and SOC teams analyze abnormal behavior in the network traffic and incident reports in order to

detect ongoing infection. IRs are converted into collection tasks on the basis of Indicators of Compromise, and monitoring of dark web forums. Malware samples for the reverse engineering, threat intelligence report about WannaCry impact, network logs to study its spread and monitor the dark web to see if they pay the ransom.

Processing

The information collected during the WannaCry attack has to be processed and filtered to transform raw intelligence into actionable insights. Some key actions like removing irrelevant or duplicate data, for example, redundant network logs and false positives by malware detection systems. Identifying the spread and encryption process of WannaCry infections can be attained by correlating its attack patterns. In order to make sharing intelligence simple, it's crucial to format intelligence into structured reports using standard formats such as STIX/TAXII to ventilate WannaCry's tactics, techniques and procedures (TTPs). For automated threat detection to data requirements include standardized reports, correlation matrices that correlate WannaCry activity with its attack lifecycle, and analysis from past decryption attempts which may inform possibilities on recovery.

Analysis & Production

The Analysis & Production is generated based on the intelligence collected on the WannaCry attack. The key actions of this work include discriminating against the WannaCry attack pattern, confirming the exploitation of EternalBlue and accounting for the system self-propagation mechanism. It is critical to assess vulnerabilities on unpatched Windows systems especially in hospitals, which were particularly exposed. Its code structure is analyzed and Ransomware as a Service (RaaS) models are investigated in order to detect future variations of WannaCry. Intelligence findings determine mitigation strategies by evaluating the effectiveness of patch deployment and proactively monitoring the network. They include IoCs, an attack technique mapping from the MITRE ATT&CK framework and the risk report including the economic impact of WannaCry.

Dissemination

The relevant stakeholders are provided with intelligence regarding WannaCry attack. The key actions involve ensuring the appropriate intelligence is received by the right people timely, sending technical intelligence to SOC teams and strategic intelligence to CISOs for policy changes. Regular compliances and speeding threats advisories are imperative together with utilizing usually commuter cybersecurity communication channels. It helps targeting critical infrastructure that are of higher threat severity. You keep a feedback loop so that you can continue to update on new findings and WannaCry variants.

Utilization

The WannaCry attack has been used to bring intelligence and apply in the phase to improve security measures. There are key actions to ensure such as deploying MS17-010 patch on all the Windows systems or to apply patches and security updates. Network monitoring enhancement

would include setting IDS/IPS to detect SMB exploits and applying honeypots to study variants of the WannaCry. Employees need to be educated to know what a phishing attempt is, how to prevent it, and should develop ransomware response plans including offline backups, and rapid containment strategies. (Chesti et al., 2020, p. 3) underscored "Following approaches can help in restricting the attack and destruction that can be caused by ransomware: 'Back up, gaining knowledge by training, using email security and spam filters, avoid clicking on unconfirmed links, never open untrusted email attachments, the download should be done only from trusted sites, avoid giving out personal data, always keep your system up to date, while using public Wi-Fi make use of VPN, use security software, drop-and-roll, know the risk, develop suitable policies, and organization best practices for users.'"

Malware Analysis

(Gallegos-Segovia et al. 2017, p.2) discuss the role of social engineering in ransomware attacks, emphasizing how malicious code is deconstructed to analyze the algorithms it employs. While this method is commonly used, it requires expertise in the programming language in which the malware was developed. The study highlights the significance of understanding these techniques to enhance cybersecurity measures and mitigate ransomware threats. The purpose of malware analysis is to understand the attack cycle.

File Information:

Name: 72406ec12b191d2fa211cf1899e62c9257379d5bdd1d850c66cc546685f3d8ea.exe

Hash: MD5: ecf4ccc75a4d40f2b70f3e05b4f0695c

Size: 2.18 MB

Type: Win32 EXE

Creation Date: 2011-12-20 09:03:08

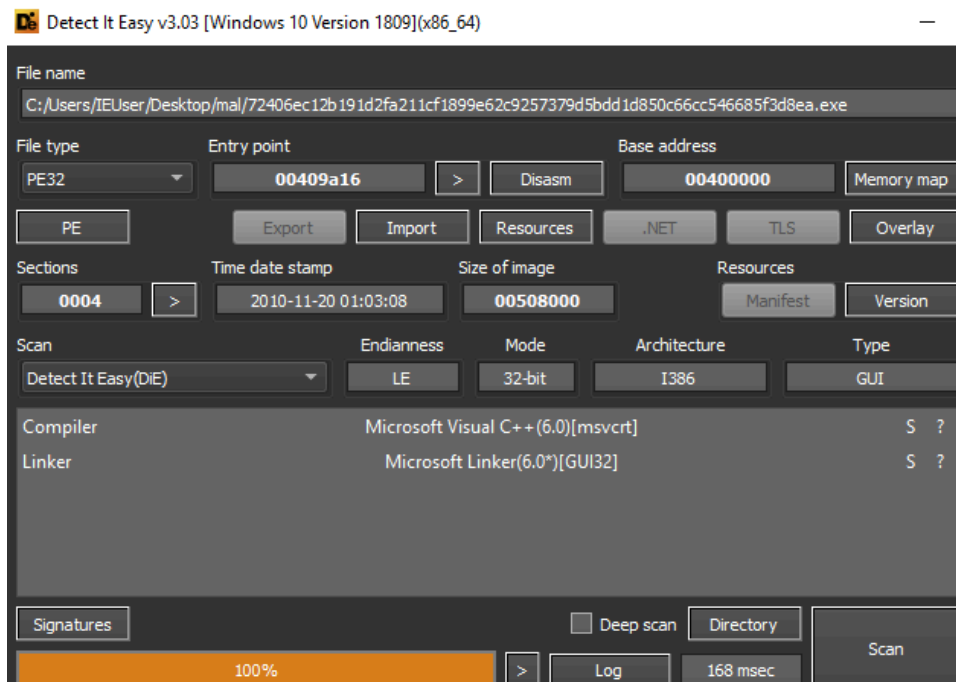
Format: PE32

Code Inspection:

Tools Used:

DIE (Detect It Easy): Used for basic file analysis and to identify the file format.

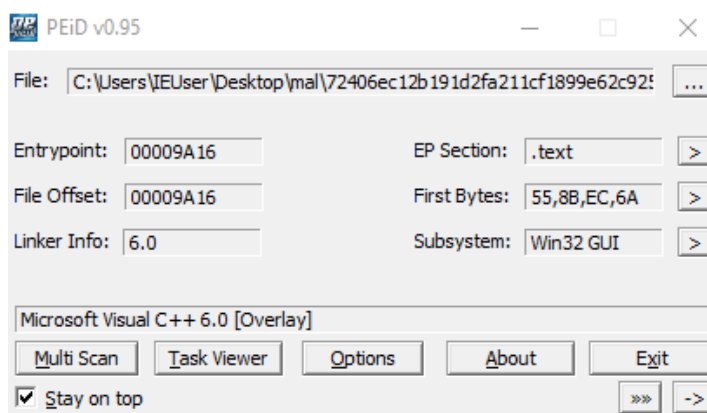
Figure 2 Detect It Easy



Note. In figure 2, we could analyse that there are 4 sections and File type is PE32. The compiler used by the malware writer is Microsoft Visual C++ 6.0 Version.

PEiD: Used for detecting packed code.

Figure 3 PEiD



Note. From figure 2 and 3, we could compare what the tools have detected and we could see that both DIE and PEiD have the same results; it means that there is no inconsistency. We could rely on the data.

IDA Pro: Used for disassembling and analyzing the code.

Figure 4 CreateServiceA

```

sub     esp, 104h
lea     eax, [esp+104h+Buffer]
push    edi
push    offset FileName
push    offset Format ; "%s -m security"
push    eax           ; Buffer
call    ds:sprintf
add     esp, 0Ch
push    0F003Fh       ; dwDesiredAccess
push    0             ; lpDatabaseName
push    0             ; lpMachineName
call    ds:OpenSCManagerA
mov     edi, eax
test    edi, edi
jz      short loc_407CCA
push    ebx
push    esi
push    0             ; lpPassword
push    0             ; lpServiceStartName
push    0             ; lpDependencies
push    0             ; lpdwTagId
lea     ecx, [esp+120h+Buffer]
push    0             ; lpLoadOrderGroup
push    ecx           ; lpBinaryPathName
push    1             ; dwErrorControl
push    2             ; dwStartType
push    10h           ; dwServiceType
push    0F01FFh       ; dwDesiredAccess
push    offset DisplayName ; "Microsoft Security Center (2.1) Service
push    offset ServiceName ; "mssecsvc2.1"
push    edi           ; hSCManager
call    ds:CreateServiceA
mov     ebx, ds:CloseServiceHandle

```

Note. In figure 4, function sub_407C40 create a service for malware.exe -m security which will run the same .exe file but with some *arguments.

Figure 4.1 Lockit

```

mov     [esi+1], al
mov     [esi+8], bl
call    ??2@YAPAXI@Z      ; operator new(uint)
mov     edi, eax
add     esp, 4
lea     ecx, [esp+10h+arg_4]
mov     ebp, edi
mov     [edi+4], ebx
mov     dword ptr [edi+14h], 1
call    ds:??0_Lockit@std@@QAE@XZ ; std::_Lockit::_Lockit(void)
cmp     dword ptr FileName+118h, ebx
jnz     short loc_408259
mov     dword ptr FileName+118h, edi
mov     [edi], ebx
mov     ecx, dword ptr FileName+118h
xor     ebp, ebp
mov     [ecx+8], ebx

loc_408259:
; CODE XREF: sub_408200+44↑j
mov     ecx, dword ptr FileName+114h
inc     ecx
mov     dword ptr FileName+114h, ecx
lea     ecx, [esp+10h+arg_4]
call    ds:??1_Lockit@std@@QAE@XZ ; std::_Lockit::~~_Lockit(void)
cmp     ebp, ebx
jz      short loc_40827D
push    ebp                ; Block
call    sub_4097FE
add     esp, 4

loc_40827D:
; CODE XREF: sub_408200+72↑j
mov     edi, dword ptr FileName+118h
push    18h                ; unsigned int
call    ??2@YAPAXI@Z      ; operator new(uint)
mov     [eax+4], edi

```

Note. This function seems to handle memory allocation and object initialization for linked lists or data structures. It uses operator new to allocate memory and set up the pointers, and manipulate a globally available file related structure (FileName + 118h and FileName + 114h).

Code Structure & Sections:

PE Header Information:

Section 1: .text - contains executable code

Section 2: .data - contains initialized data variables

Section 3: .rsrc - contains resources

Section 4: .rdata - Contains read-only data

Main Code

Figure 5 Start Function [Main Entry]

```
start proc near
Code= dword ptr -78h
var_74= dword ptr -74h
var_70= byte ptr -70h
var_6C= dword ptr -6Ch
var_68= dword ptr -68h
var_64= byte ptr -64h
var_60= byte ptr -60h
StartupInfo= _STARTUPINFOA ptr -5Ch
ms_exc= CPPEH_RECORD ptr -18h

push    ebp
mov     ebp, esp
push    0FFFFFFFh
push    offset stru_40A1A0
push    offset _except_handler3
mov     eax, large fs:0
push    eax
mov     large fs:0, esp
sub     esp, 68h
push    ebx
push    esi
push    edi
mov     [ebp+ms_exc.old_esp], esp
xor     ebx, ebx
mov     [ebp+ms_exc.registration.TryLevel], ebx
push    2 ; Type
call    ds:__set_app_type
pop     ecx
or      dword_70F894, 0FFFFFFFh
or      dword_70F898, 0FFFFFFFh
call    ds:__p__fmode
mov     ecx, dword_70F88C
mov     [eax], ecx
call    ds:__p__commode
mov     ecx, dword_70F888
mov     [eax], ecx
mov     eax, ds:adjust_fdiv
mov     eax, [eax]
mov     dword_70F890, eax
call    nullsub_1
cmp     dword_431410, ebx
jnz     short loc_409A99
```

Note. In figure 5, Initial setup and system checks are typically performed in the start function for ransomware. This function takes care of exception handling, runtime configurations and so on, and may also create or modify crucial variables. This could be the preparation for file encryption, the process of setting up communication with a C2 server or just preparing the system for execution of malicious payloads.

Code Obfuscation/Encryption:

Signs of Obfuscation: Strings like `tasksche.exe`, and <http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwff.com> may be dynamically constructed, hinting at potential obfuscation or runtime decoding.

Control Flow Obfuscation: Presence of dynamic imports and external DLL loading suggests some runtime manipulation like `??1_Lockit@std@@@QAE@XZ`, `launcher.dll`, `connect` and many others

Suspicious API Calls: Some of the suspicious API Calls are CryptGenRandom, InternetOpenURLA, GetAdaptersInfo, QueryPerformanceFrequency, RegisterServiceCtrlHandlerA.

Hardcoded Strings:

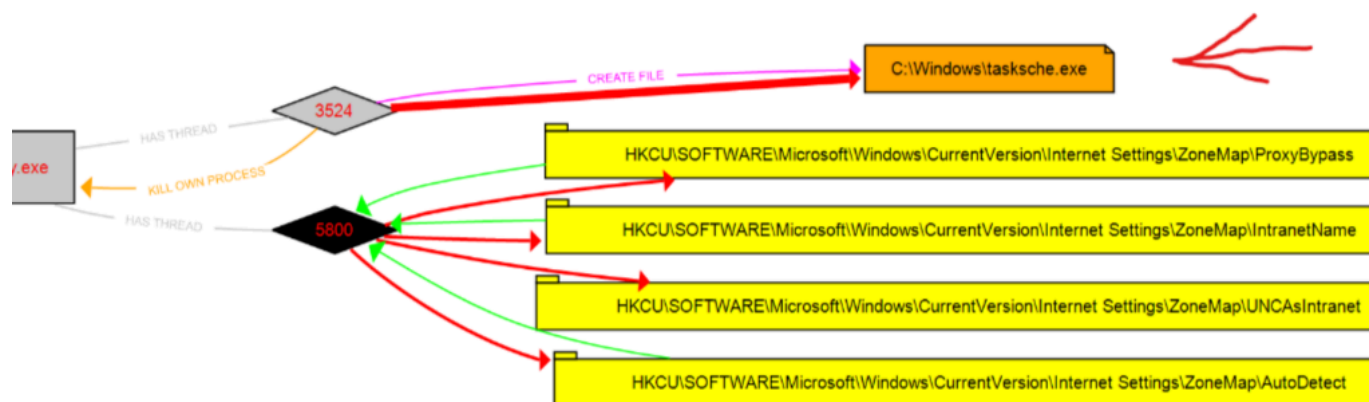
File Paths:

“C:\\%s\\%s”: Used to construct a file path.

“WINDOWS”: Used as part of the file path.

“taskshe.exe”: Name of the executable that the ransomware attempts to create or manipulate.

Figure 6 Procdot32



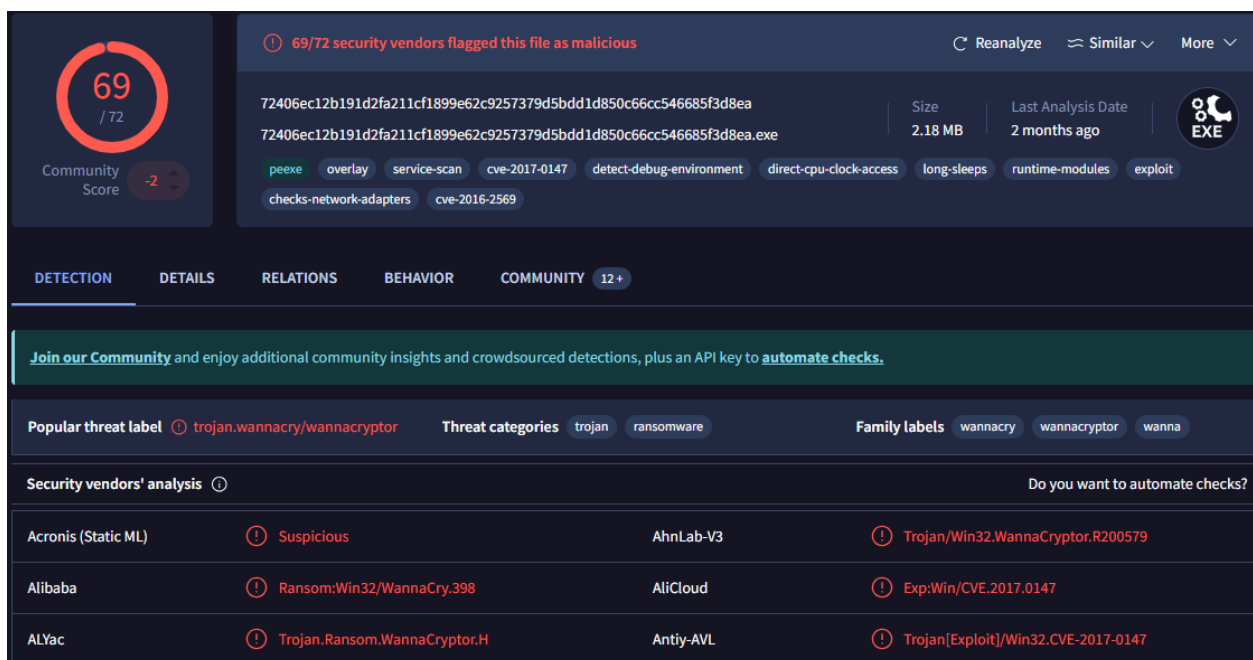
Note: In figure 6, the diagram has been taken from procdot, it takes csv file as an input of procmon and illustrates what the malware has been doing with the system. As we can see through the arrow a child process of wannacey.exe has been created named tasksche.exe which is a known malicious file.

Strings: The strings used from these dlls are “WS2_32.dll”, “iphlpapi.dll” and “WININET.dll”.

Signatures: VirusTotal Analysis

Total Detections: 69/72 engines detected

Figure 7 VirusTotal



Note: The VirusTotal is a famous website which takes Hashes and shows us if there is any malware related to it. The malware I have selected for analysis is the same as the WannaCry 2017 attack as we have the tags which are more relatable to it.

Dynamic Analysis Report

This structure focuses on debugging a malware sample using x32dbg to analyze its behavior at the assembly level.

Environment

Analysis System:

Operating System: Windows 10 x64 VM

Debugger Used: x32dbg

Additional Tools: Process Monitor and Process Hacker

Network Connectivity: Internet Access

Loading the Malware in x32dbg

Initial Analysis:

MD5 Hash: ecf4ccc75a4d40f2b70f3e05b4f0695c

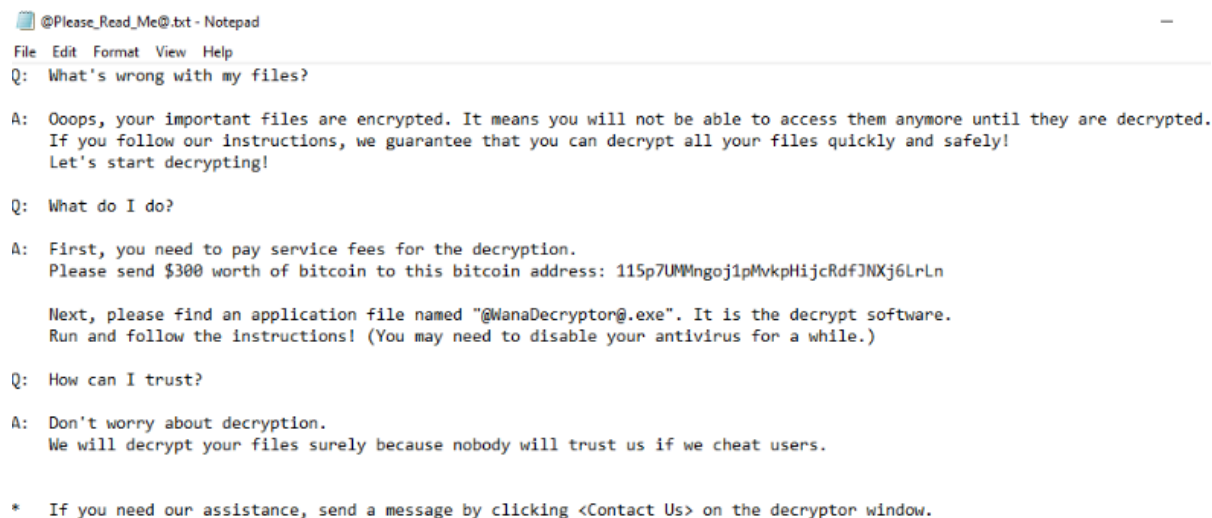
File Type: PE32 Executable

Loaded Modules: WS2_32.dll, iphlapi.dll and WININET.dll

Figure 8 Internet connected to VM machine



Note. In figure 8 the internet was connected to my VM, so after running the malware.exe file there was a pop up of files encrypted.

Figure 9 Readme


```

@Please_Read_Me@.txt - Notepad
File Edit Format View Help
Q: What's wrong with my files?

A: Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.
If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely!
Let's start decrypting!

Q: What do I do?

A: First, you need to pay service fees for the decryption.
Please send $300 worth of bitcoin to this bitcoin address: 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Next, please find an application file named "@WanaDecryptor@.exe". It is the decrypt software.
Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q: How can I trust?

A: Don't worry about decryption.
We will decrypt your files surely because nobody will trust us if we cheat users.

* If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.

```

Note. The figure 9 tells us what has happened to our files and what we need to do to decrypt our files.

Entry Point Analysis:

Address of Entry Point (OEP): 0x00009A16

Instruction at OEP: PUSH EBP

Suspicious Instructions at Start: mov EAX, ds:_adjust_fdiv as can s in figure 10.

Figure 10 Floating-point operations

00409A74	A1 E4A04000	mov eax,dword ptr ds:[<&_adjust_fdiv>]
00409A79	8B00	mov eax,dword ptr ds:[eax]
00409A7B	A3 90F87000	mov dword ptr ds:[70F890],eax

Note. Some malware manipulates floating-point operations to detect virtual machines or debugging environments.

Debugging & Execution Flow

Figure 11 Breakpoint on suspicious Calls

Type	Address	Module/Label/Exception	State	Disassembly
Software				
	743C55F0	<iphlpapi.dll.GetAdaptersInfo>	Enabled	mov edi,edi
	743DC380	<iphlpapi.dll.GetPerAdapterInfo>	Enabled	mov edi,edi
	74718180	<wininet.dll.InternetOpenA>	Enabled	mov edi,edi
	74738000	<wininet.dll.InternetCloseHandle>	Enabled	mov edi,edi
	747F7E10	<wininet.dll.InternetOpenUrlA>	Enabled	mov edi,edi
	751DDFF0	<advapi32.dll.CryptAcquireContextA>	Enabled	mov edi,edi
	751DE8F0	<advapi32.dll.CryptGenRandom>	Enabled	mov edi,edi
	76864AC0	<ws2_32.dll.htonl>	Enabled	mov edi,edi
	76865380	<ws2_32.dll.select>	Enabled	push 58
	76865650	<ws2_32.dll.connect>	Enabled	mov edi,edi
	76865750	<ws2_32.dll.send>	Enabled	mov edi,edi
	76868FA0	<ws2_32.dll.socket>	Enabled	mov edi,edi
	7686EAC0	<ws2_32.dll.closesocket>	Enabled	mov edi,edi
	76871460	<ws2_32.dll.recv>	Enabled	mov edi,edi
	76871810	<ws2_32.dll.ioctlsocket>	Enabled	mov edi,edi
	768719A0	<ws2_32.dll.WSASocket>	Enabled	mov edi,edi
	76876900	<ws2_32.dll.inet_addr>	Enabled	mov edi,edi
	768769F0	<ws2_32.dll.htons>	Enabled	mov edi,edi
	76876E00	<ws2_32.dll.inet_ntoa>	Enabled	mov edi,edi

Note. I have set breakpoints on wininet.dll, ws2_32.dll, and iphlapi.dll because they are commonly exploited by malware for network-related activities.

Execution Analysis: Step-by-Step Execution Observations

Instruction Sequence: [CALL InternetOpenA -> PUSH lpszAgent -> PUSH dwAccessType -> PUSH lpszProxy -> PUSH lpszProxyBypass -> PUSH dwFlags -> CALL InternetOpenA -> MOV EAX, return_value -> TEST EAX, EAX]

Figure 12 LdrpInitializeProcess

8180	mov edi,edi	InternetOpenA
8182	push ebp	
8183	mov ebp,esp	
8185	sub esp,64	
8188	mov eax,dword ptr ds:[748A32F0]	
818D	xor eax,ebp	
818F	mov dword ptr ss:[ebp+4],eax	
8192	mov eax,dword ptr ss:[ebp+8]	
8195	push ebx	
8196	mov dword ptr ss:[ebp+28],eax	
8199	mov eax,dword ptr ss:[ebp+14]	
819C	push esi	
819D	push edi	
819E	mov dword ptr ss:[ebp+24],eax	
81A1	lea edi,dword ptr ss:[ebp+18]	
81A4	mov esi,dword ptr ss:[ebp+C]	
81A7	xor eax,eax	
81A9	mov ebx,dword ptr ss:[ebp+10]	
81AC	and dword ptr ss:[ebp+1C],0	
81B0	stosd	
81B1	push 3C	
81B3	push 0	
81B5	stosd	
81B6	stosd	
81B7	stosd	
81B8	stosd	
81B9	lea eax,dword ptr ss:[ebp+64]	[ebp+64]:&"ALLUSERSPROFILE=C:\\ProgramData"
81BC	push eax	
81BD	call <JMP.&memset>	
81C2	add esp,C	
81C5	and dword ptr ss:[ebp+20],0	
81C9	test byte ptr ds:[748A3950],2	
81D0	jne wininet.747A889F	
81D6	lea ecx,dword ptr ss:[ebp+64]	[ebp+64]:&"ALLUSERSPROFILE=C:\\ProgramData"

Note. This is a part of a function called LdrpInitializeProcess within the Windows loader which initializes a process. It prepares local buffer and sets up the stack frame and stores function

arguments. memset implies memory initialization; these subsequent function calls may point to network related activity (wininet.74E9B954).

Register Changes:

EAX: Value before: 0019FFCC and after execution: 00402F0

EBX: Value before: 003B2000 and after execution: 00000000

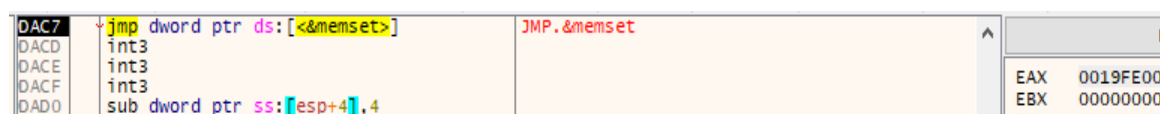
ESP: Value before: 0019FF74 and after execution: 0019FE68

Code Unpacking:

Signs of packing: YES, due to presence XOR-based obfuscation

OEP Recovery Details: The OEP is likely recovered when execution jumped to the memory region starting at 0x0019FE00, indicated by the CALL dword ptr ds:[<&memset>] instruction.

Figure 13 Original Entry Point



Note. This CALL dword ptr ds:[<&memset>] instruction, by my understanding, indicates that execution jumps to the memory region which starts at 0x0019FE00 and has the OEP probably recovered, likely. A jump of this kind usually indicates the point where unloading is over and the original executable code is loaded, and it is an OEP recovery point.

Memory Analysis

Suspicious Memory Allocations

Figure 14 Heap Modification

```

768262E0 $ push 1C GlobalAlloc
768262E2 push kernelbase.768C20F8
768262E7 call kernelbase.7683459C
768262EC xor esi,esi
768262EE mov dword ptr ss:[ebp-1C],esi
768262F1 mov dword ptr ss:[ebp-24],esi
768262F4 mov ebx,dword ptr ss:[ebp+8]
768262F7 test ebx,FFFF808D
768262FD jne kernelbase.768509EA
76826303 mov ecx,ebx
76826305 shr ecx,3
76826308 and ecx,8
7682630B mov dword ptr ss:[ebp-28],ecx
7682630E test b1,2
76826311 je kernelbase.768263FA
76826317 mov edi,esi
76826319 mov dword ptr ss:[ebp-20],edi
7682631C push dword ptr ds:[768D57D4]
76826322 call dword ptr ds:[<&RtlLockHeap>]
76826328 mov dword ptr ss:[ebp-4],esi
7682632B mov dword ptr ss:[ebp-4],1
76826332 push esi
76826333 push kernelbase.768D57E0
76826338 call dword ptr ds:[<&RtlAllocateHandle>]
7682633E mov esi,eax
76826340 mov dword ptr ss:[ebp-1C],esi
76826343 test esi,esi
76826345 je kernelbase.76850A1A
76826348 lea eax,dword ptr ds:[esi+4]
7682634E mov dword ptr ss:[ebp-24],eax
76826351 cmp dword ptr ss:[ebp+C],edi
76826354 je kernelbase.76826399
76826356 push dword ptr ss:[ebp+C]
76826359 mov eax,dword ptr ds:[768D56C0]
7682635E add eax,100000
76826363 or eax,dword ptr ss:[ebp-28]
76826366 or eax,301

```

Note. The program is interacting with RtlLockHeap, RtlAllocateHandle, and RtlAllocateHeap functions. The add EAX, 100000 instruction indicates that the allocated memory address in EAX is being adjusted by 1MB. This suggests the malware is preparing a large memory region for storing malicious code.

Dumping Decrypted Code

Dump Method Used: Scylla Plugin

Recovered PE Header: YES

Figure 15 Dump.exe File

File name C:/Users/IEUser/Desktop/mal/72406ec12b191d2fa211cf1899e62c9257379d5bdd1d850c66cc546685f3d8ea_dump.exe					
File type PE32	Entry point 00409a16	>	Disasm	Base address 00400000	Memory map
PE	Export	Import	Resources	.NET	TLS
Overlay					
Sections 0004	>	Time date stamp 2010-11-20 01:03:08	Size of image 00508000	Resources Manifest	Version
Scan Detect It Easy(DiE)	Endianness LE	Mode 32-bit	Architecture I386	Type GUI	
Compiler	Microsoft Visual C++ (6.0)[msvcrt]				S ?
Linker	Microsoft Linker(6.0*)[GUI32]				S ?

Note. The logged decryption code is the output from the Scylla Plugin, which is useful to bypass anti debugging techniques, and then extract executable code after it has been unpacked. I then dumped the code with another tool and verified the PE header recovery with DIE (Detect It Easy), which proved to me that the unpacked executable is uncompromised and has its structure fixed.

SHA256 of Dumped Executable:

BAA0B0E8F1D73D70CC8EF20A1DB7F89F4F12595551BB1C26F37D2B4A68646688

API Calls & Functionality

API Calls Used: The API Calls used are GetAdaptersInfo, GetPerAdapterInfo, InternetOpenA, Internet CloseHandle, InternetOpenURLA, CryptAcquireContextA, CryptGenRandom, Htonl, Select, Connect, Send, Socket, Closesocket, Recv, Ioctlsocket, WSASStartup, Inet_addr, Htons, Inet_ntoa.

Process Injection Analysis:

Injected Target Process: svchost.exe and Explorer.EXE

Injection Method: LoadLibraryExW

Calls Used for Injection: <&RtlInitUnicodeStringEx>, <&LdrGetDllPath> and <&RtlReleasePath>

Figure 16 LoadLibraryExW

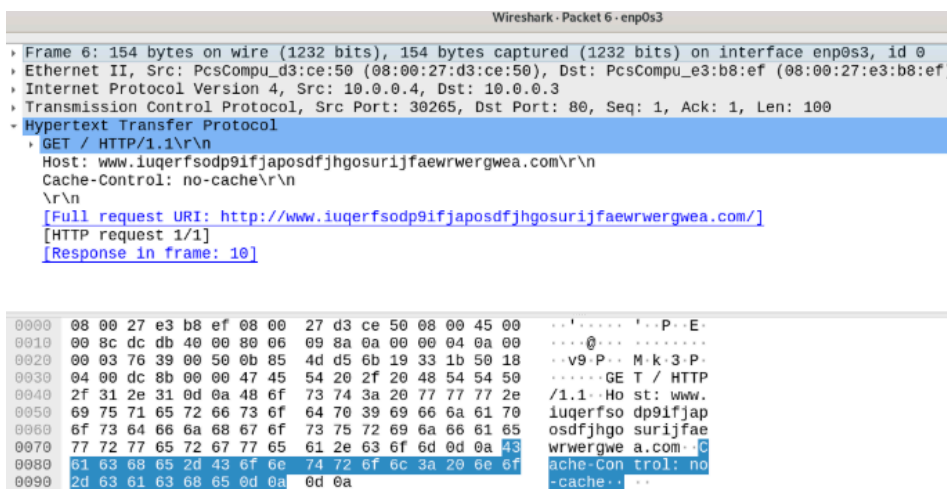
74858B90	\$	mov edi,edi	LoadLibraryExW
74858B92		. push ebp	
74858B93		. mov ebp,esp	
74858B95		. and esp,FFFFFFF8	
74858B98		. mov eax,dword ptr ss:[ebp+8]	
74858B9B		. sub esp,1C	
74858B9E		. push ebx	ebx:L"api-ms-win-core-synch-11-2-0"
74858BA0		. push esi	
74858BA1		. push edi	
74858BA3		. test eax,eax	
74858BA9		. je kernelbase.74858CE3	
74858BAD		. cmp dword ptr ss:[ebp+C],0	
74858BB3		. jne kernelbase.74858CE3	
74858BB6		. mov ebx,dword ptr ss:[ebp+10]	ebx:L"api-ms-win-core-synch-11-2-0"
74858BBC		. test ebx,FFFF0000	ebx:L"api-ms-win-core-synch-11-2-0"
74858BC2		. jne kernelbase.74858CE3	42: 'B'
74858BC4		. mov esi,ebx	
74858BC7		. and esi,42	
74858BCA		. cmp esi,42	
74858BD0		. je kernelbase.74858CE3	
74858BD1		. push eax	
74858BD5		. lea eax,dword ptr ss:[esp+24]	
74858BD6		. push eax	
74858BD6		. call dword ptr ds:[<&RtlInitUnicodeStri	

Note. I conclude that the target processes to inject are svchost.exe and Explorer.EXE, as these are both common system processes that often are used for process injection. To understand how

the malware shifts and manages its malicious code to these processes, the calls `<&RtlInitUnicodeStringEx>`, `<&LdrGetDllPath>`, and `<&RtlReleasePath>` were tracked when malicious DLL was loaded using the injection method `LoadLibraryExW`.

Network Analysis:

Figure 17 HTTP Request



Note. In figure 17, the malware sent a request to an unknown website and was successful. After reaching the website the ransomware terminated directly.

Anti-Analysis Technique Observed

Figure 18 Using the function `IsDebuggerPresent` to identify debugger existence.

```

.text:004016CB
.text:004016CB loc_4016CB:                                ; CODE XREF: sub_401660+3E1j
.text:004016CB      fld      db1_431450
.text:004016D1      fcomp   ds:db1_40A188
.text:004016D7      fnstsw  ax
.text:004016D9      test   ah, 40h
.text:004016DC      jz      short loc_40171C
.text:004016DE      lea     eax, [esp+1Ch+Frequency]
.text:004016E2      push   eax                ; lpFrequency
.text:004016E3      call   ds:QueryPerformanceFrequency
.text:004016E9      test   eax, eax
.text:004016EB      jnz     short loc_40170C
.text:004016ED      mov     eax, 4318DE83h
.text:004016F2      imul    esi
.text:004016F4      sar     edx, 12h
.text:004016F7      mov     ecx, edx
.text:004016F9      shr     ecx, 1Fh
.text:004016FC      add     edx, ecx
.text:004016FE      push   edx                ; dwMilliseconds
.text:004016FF      call   ds:Sleep
.text:00401705      pop     edi
.text:00401706      pop     esi
.text:00401707      pop     ebx
.text:00401708      add     esp, 10h
.text:0040170B      retn

```

Note. In figure 18, the function is checking if there is any debugger present or not. Query Performance Frequency checks the system's high resolution timer and calculates delay and calls sleep to slow execution in any debugger.

Conclusion

Most impactful of cyber incidents in 2017 that made use of the EternalBlue vulnerability to spread rapidly across unpatched Windows systems was WannaCry attack. For understanding of WannaCry's attack lifecycle, adversary motives and mitigation strategies this report used the Threat Intelligence Cycle. WannaCry gained global visibility through a number of intelligence findings such as poor patch management, outdated systems and lack of proactive cybersecurity measures. Financial institutions, the NHS, and government agencies were severely disrupted for years without applying security updates in a timely manner and proved the risk.

Key aspects in identifying and mitigating through Indicators of Compromise, adversary tactics and measures is threat intelligence. Despite that, the problem of attribution of cyber attacks to certain actors, the lack of sharing and collaboration between private and government as well as the lack of threat intelligence remain challenges of current threat intelligence solutions. However, the WannaCry attack highlighted the importance of cybersecurity awareness, automation of threat detection and defensive strategies. (Popoola et al., 2017, p. 5) noted that "Kaspersky Lab and Intel have joined forces with Interpol and the Dutch National Police to set up a website (www.nomoreransom.org) aimed at helping people to avoid falling victim to ransomware".

Recommendations

Cost effective strategies that an organization can follow to prevent future WannaCry like ransomware attacks are prevention strategies. However, first hand recommendations include automating the deployment of patches to ensure the system stays up to date, the use of network segmentation to prevent lateral propagation, and the use of the most advanced endpoint detection response (EDR) systems to catch out our own contractor, early ransomware related behavior. The threat of phishing-based ransomware infection would also be removed through regular cybersecurity training to employees. There would be greater cyber threat information exchange between governments and enterprises which would help in planning ahead and take action accordingly.

The progress does not solve all problems of cyber threat intelligence. However, passive information sharing of real time threat intelligence is restricted by lack of uniform threat intelligence frameworks. This makes it difficult for prevention of quickly spreading ransomware attacks. Additionally, cybercriminals remain betting on advanced tactics such as Ransomware as a Service (RaaS) and double extortion, preserving defense planning.

References

- Wikipedia contributors. *WannaCry ransomware attack*. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack#United_Kingdom
- Avast Software. (n.d.). *What is hospital ransomware?* Avast. <https://www.avast.com/business/resources/what-is-hospital-ransomware#pc>
- Gabr, M. (n.d.). *WannaCry analysis*. 0xg4br. <https://0xg4br.github.io/malware%20analysis/WannaCry/>
- European Union Agency for Cybersecurity (ENISA). (2024). *ENISA Threat Landscape 2024*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- Popoola, S. I., Iyekepolo, U. B., Ojewande, S. O., Sweetwilliams, F. O., John, S. N., & Atayero, A. A. (2017). Ransomware: Current trend, challenges, and research directions. *ResearchGate*. https://www.researchgate.net/publication/320346114_Ransomware_Current_Trend_Challenges_and_Research_Directions
- Meurs, T., Junger, M., Tews, E., & Abhishta, A. (2023). Ransomware: How attacker's effort, victim characteristics, and context influence ransom requested, payment, and financial loss. *ResearchGate*. https://www.researchgate.net/publication/367295305_Ransomware_How_attacker%27s_effort_victim_characteristics_and_context_influence_ransom_requested_payment_and_financial_loss
- Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017). Social engineering as an attack vector for

ransomware. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 3262-3267). IEEE. <https://ieeexplore.ieee.org/document/8229528>

Temara, S. (2024). The ransomware epidemic: Recent cybersecurity incidents demystified. *Asian Journal of Advanced Research and Reports*, 18(3), 1-16. <https://journalajarr.com/index.php/AJARR/article/view/610>

Trautman, L. J., & Ormerod, P. C. (2019). WannaCry, ransomware, and the emerging threat to corporations. *Tennessee Law Review*, 86(3), 503-556. [Wannacry, Ransomware, and the Emerging Threat to Corporations by Lawrence J. Trautman, Peter Ormerod :: SSRN](https://www.ssrn.com/sol3/papers.cfm?abstract_id=3488888)

Prasad, K. D. S., & Kumar, P. H. R. (2024). A systematic study on ransomware attack: Types, phases, and recent variants. *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. IEEE. <https://ieeexplore.ieee.org/abstract/document/10511218>

Srivastava, K., Faist, K., Lickert, B., Neville, K., McCarthy, N., Fehling-Kaschek, M., & Stolz, A. (2024). Assessment of the impact of cyber-attacks and security breaches in diagnostic systems on the healthcare sector. *IEEE*. <https://ieeexplore.ieee.org/document/10679475>

Albshaier, L., Almarri, S., & Rahman, M. M. H. (2024). Earlier decision on detection of ransomware identification: A comprehensive systematic literature review. *Information*, 15(8), 484. <https://doi.org/10.3390/info15080484>

Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. Z. (2020). Evolution, mitigation, and prevention of ransomware. In *Proceedings of the 2020 2nd International Conference on Computer and Information Sciences (ICCIS)* (pp. 1-6). IEEE. <https://doi.org/10.1109/ICCIS49240.2020.9257708>

Ansori, A., Damyati, F., & Dhestyani, S. A. (2024). Mitigation of malware ransomware virus. *MATICS: Jurnal Ilmu Komputer dan Teknologi Informasi*, 16(2), 76-83. <https://doi.org/10.18860/mat.v16i2.28794>

Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*. <https://doi.org/10.1016/j.iotcps.2023.12.001>