Evil Corp WastedLocker Ransomware

September 2020

Cyberint

TABLE OF CONTENTS

INTRODUCTION

This report provides an overview of 'WastedLocker', reportedly the ransomware threat used in the recent Garmin incident, along with the commonly observed infection vector so that organizations can assess the preparedness of their defenses against threats of this nature.

As is common with groups operating out of Russia or the Commonwealth of Independent States (CIS), organizations targeted by Evil Corp with WastedLocker have come from a variety of industries and most are located within the United States. Whilst there are reports of organizations being targeted within Europe, it is suggested that these may be US-based operations.

Garnering widespread press coverage, an 'outage' affecting the avionics, GPS receiver and wearable technology manufacturer Garmin in July 2020 [1], based on information provided by several people with 'inside' knowledge, is thought to be a consequence of an attack in which the WastedLocker ransomware was deployed. Subsequently, a reported USD 10 million ransom demand was paid to the operators of 'WastedLocker', widely attributed as being the cybercriminal gang known as 'Evil Corp', resulting in Garmin receiving a working decryption key resulting in the restoration of their data.

Assuming Evil Corp are indeed responsible for WastedLocker, as widely attributed albeit a fact deemed inconclusive by Arete Incident Response, the incident response company tasked with assisting Garmin, financial sanctions imposed by the United States (US) in December 2019 would have precluded any legal payment and, as such, it is speculated that Garmin may have made the payment via an intermediary.

This incident yet again demonstrates the unenviable situation that victims of 'big game hunter' ransomware attacks find themselves in: either the organization remains offline whilst remediation and restoration processes are implemented, undoubtedly with mounting financial and reputational losses, or, agree to the threat actor's demands and pay the ransom to potentially be back on line in a fraction of the time.

Adding further 'encouragement' to make ransom payments, those responsible for these attacks appear to be fully adept at understanding the costs of an incident and factor this into their demands. This in turn potentially creates a situation whereby it is almost cheaper to pay the ransom rather than pay for incident response and data recovery alongside any losses whilst systems remain offline.

Unfortunately, any ransom payment likely only serves as to perpetuate the broader problem, fueling the development of more sophisticated ransomware threats and likely motivating other cybercriminals to get involved in this highly lucrative activity.

As is common with other big game hunter campaigns, those behind WastedLocker appear to use somewhat sophisticated tactics, techniques, and procedures (TTP) to gain access to a victim organization and ascertain which systems should be encrypted for maximum effect.

Notably, and unlike other campaigns conducted by groups such as 'Maze' and 'REvil', WastedLocker does not appear to employ the 'steal, encrypt and leak' tactic although this would be well within their capabilities should they decide to in the future.

KEY POINTS

- Initial infection vector utilizes compromised websites with the SocGholish social engineering framework to deliver fake 'update' alerts.
- Potential compromise of existing Dridex victims.
- CobaltStrike dropped onto potential victim machines to determine viability for ransomware attack.
- Modular WastedLocker ransomware threat allows customization for each victim organization.
- Privilege escalation routine makes use of NTFS alternate data streams to bypass User Account Control.
- Typical ransomware functionality including deletion of volume shadow copies along with the reconfiguration of Windows Defender and Firewall.
- In-memory encryption of files to evade end-point security solutions using behaviors analytics.
- Ransoms range from USD 0.5 to 10 million, payable in Bitcoin.

EVIL CORP

Believed to have been active since at least 2011, Evil Corp are a Russia-based organized cybercriminal group allegedly led by a Russian citizen named 'Maksim Viktorovich Yakubets', also known as 'Aqua' and 'Aquamo', alongside at least sixteen other individuals that are responsible for the logistic, technical and financial functions within the cybercriminal organization.

Described as one of the world's most prolific cybercriminal organizations, Evil Corp are responsible for countless campaigns in which 'Dridex' variants (also known as 'Bugat' and 'Cridex') and 'JabberZeus' were distributed. These banking threats were typically used to steal account credentials that would facilitate access and enable the group to make fraudulent transfers resulting in the theft of millions from victims throughout Europe and the United States).

Having stolen funds from victims, the well-structured group recruited money mules worldwide, often using seemingly legitimate 'work from home' job offers for 'money transfer agents', that would then receive and transfer stolen funds to accounts under the control of Evil Corp members.

In addition to banking threats, Evil Corp are reportedly responsible for the 'BitPaymer' ransomware threat, prevalent since 2017, as well as being potentially linked to the ransomware-as-a-service variant 'DoppelPaymer' that was released in 2019. Seemingly drawing upon this experience, 'WastedLocker' was first observed in May 2020 having reportedly been in development for some months prior.

As is consistent with an organized cybercriminal group, skilled exploit writers and developers are responsible for constantly evolving their threats to thwart endpoint security solutions as well as making updates whenever their malware is detected. It is also reported that, to aid in the development of threats that can bypass common security solutions, the group have abused victim email accounts to interact with security vendors, posing as potential sales leads and requesting trial versions of products that can then be assessed against their malware.

INDICTMENTS/SANCTIONS

To disrupt the activity of Evil Corp, Maksim Viktorovich Yakubets and an alleged key figure named 'Igor Olegovich Turashev' were named in indictments filed by the US Department of Justice (DOJ) in December 2019. In addition to offering a USD 5 million reward for information leading to their arrest and/or conviction of these two individuals, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) designated them, along with other group members and related businesses, as being subject to financial sanctions.

Given these sanctions, any individual or organization under US jurisdiction would be compelled to comply and not knowingly conduct business with, or make financial payments to, Evil Corp. Failure to comply with these OFAC sanctions, such as potentially making a

ransom payment, could result in fines of up to USD 20 million and/or a custodial sentence of up to 30 years for an individual.

TACTICS, TECHNIQUES & PROCEDURES

Notably differing from many of the 'steal, encrypt and leak' targeted ransomware gangs, Evil Corp appear to focus on silently disrupting large organizations and seemingly avoiding the unnecessary attention that data theft and leaks would bring. That being said, whilst there has been no reported public exposure of data from their victims, that is not to say that data hasn't been stolen, especially when considering that the threat group could have remained undetected within a victim network for some time.

Of the known attacks linked to Evil Corp that result in the delivery of the WastedLocker ransomware threat, the following tactics, techniques and procedures (TTP) appear to be somewhat consistent although it should be noted that Evil Corp seemingly tailor their threats to specific victims.

INITIAL INFECTION VECTOR: SOCGHOLISH/DRIDEX

Whilst many big game hunter ransomware groups seek to exploit vulnerabilities in a target organization's internet-facing infrastructure, Evil Corp have used driveby exploit tactics to deliver 'fake update alerts' from compromised legitimate websites.

This somewhat indiscriminate tactic suggests that victim organizations are not targeted specifically and fall victim due to an unsuspected user accessing a weaponized website. Similar techniques could easily be utilized in a watering-hole attack by identifying and compromising websites known to be of interest to the potential victim.

Likely using some form of script injection attack, Evil Corp compromises legitimate websites for use in their drive-by attacks and makes use of 'SocGholish', a JavaScript-based social engineering framework, to profile or fingerprint the visitor and, presumably if they meet the required criteria, deliver a fake alert [Figure 1].

Figure 1 - Example fake update alert

Should the visitor fall for this social engineering attempt, they are lured into downloading a payload that masquerades as a legitimate software update. Previous use of SocGholish, a framework that was first observed in 2018 and used with a variety of commodity malware threats, has seen HTML application (HTA) files as well as ZIP archives containing scripts to deliver the next stage payload.

Notably, SocGholish methods delivering scripts may result in highly suspicious behaviors such as the execution of the downloaded script using the Windows Scripting Host, wscript.exe, from the temporary directory, %TEMP% .

Furthermore, it is suggested that some organizations have been compromised through existing Dridex infections, perhaps where Evil Corp have maintained persistence and, likely following some reconnaissance phase, determined that a victim organization would be susceptible to ransomware extortion.

RECONNAISSANCE & PERSISTENCE: COBALTSTRIKE

Cobalt Strike, a legitimate commercial tool is sold for use in red team (penetration testing) operations, provides a post-exploitation implant as well as covert channels that can be used be nefarious threat actors in their malicious campaigns.
CobaltStrike payloads observed in Evil Corp campaigns have been embedded within PowerShell scripts utilizing a common method of obfuscation and encryption, such as base64 encoding and AES encryption, to counter analysis and detection.

Notably, and potentially to address a specific security solution in place at the victim organization, a CobaltStrike loader payload has been observed as including code to detect the presence of CrowdStrike, based on the presence of a directory within

%PROGRAMFILES% , and subsequently attempts to detach the calling process from its console using the FreeConsole function, presumably in an attempt to thwart the end-point security solution.

Having successfully run, intelligence is gathered from the compromised host, determining if it is part of a larger organization, and setting the groundwork for lateral movement across the network.

Additionally, as is common with big game hunter ransomware attacks, this initial intrusion is used to perform reconnaissance to further determine the security posture of the victim organization which can then be circumvented with the delivery of subsequent threats as well as attempting to disable security software and disrupt any backup.

RANSOMWARE: WASTEDLOCKER

First observed in May 2020, and actively used since, 'WastedLocker' exhibits a few traits that are consistent with BitPaymer, an Evil Corp ransomware threat active since 2017 and seemingly now superseded, such as the use of a builder to customize the threat with victim specific details and similarities in their ransom notes. Unlike BitPaymer, WastedLocker reportedly draws upon Evil Corp's experience with Dridex and introduces modular capabilities that could facilitate further victim-specific customization or additional functionality to be added.

In addition to victim-specific customizations, WastedLocker makes use of a custom crypter, known as 'CryptOne' and previously utilized by other malware families including Gozi ISFB and Netwalker, to increase the complexity of the threat, such as introducing junk code into the malware binary, and provide anti analysis and evasion capabilities.

Rather than deploying the WastedLocker ransomware broadly within a victim network, Evil Corp are reportedly selective and focus their attentions on infrastructure that would maximize the impact such as cloud services, database servers, file servers and virtual machine hosts. Furthermore, servers that are related to customer-facing services, especially those that are revenue generating, and infrastructure related to backups are singled out for encryption.

FILE & SERVICE NAME GENERATION METHOD

Presumably to appear somewhat legitimate, and to provide variance between campaigns, WastedLocker selects random file and service names from a list that is generated by reading the names of Windows Registry keys found within HKLM\SYSTEM\CurrentControlSet\Control [Figure 2], splitting any that contain capital

letters into separate strings (for example AccessibilitySettings would result in Accessibility and Settings).

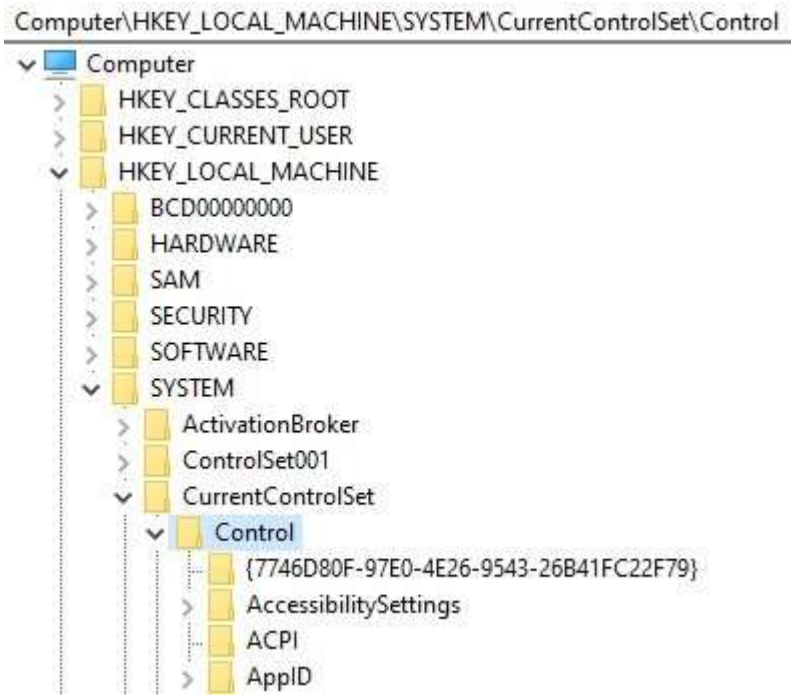

Figure 2 - Windows Registry used for file and service names

PRIVILEGE ESCALATION

It is understood that WastedLocker first attempts to run from the %SYSTEM32 directory having taken ownership of the ransomware executable using the command takeown.exe /F <filename> , should this execution fail due to a lack of administrative privileges, a User Account Control (UAC) bypass method is utilized to elevate privileges without alerting the victim to the attempt [Figure 3].

Figure 3 - Example UAC prompt

The UAC bypass method is similar to that employed by BitPaymer and attempts to make use of an alternate data stream (ADS), a feature of the Windows file system (NTFS), within which the WastedLocker ransomware can be hidden and executed in the context of a legitimate file. By default, Windows does not provide any mechanism with which to view or detect the presence of an ADS and therefore the malware will effectively be invisible to the victim.

The bypass method consists of the following steps:

- Creation of a directory within %APPDATA% using a random directory name from the generation method.
- Selection of a random executable (.exe) or dynamic link library (.dll) file from %SYSTEM32% that is then copied to %APPDATA%\<directory>.
- Creation of an alternate data stream (ADS) within the copied system file named: bin within which the ransomware will be copied.
- Creation of a directory within %TEMP%, using a random directory name from the generation method, that is set to a mount point of C:\Windows␣ (where ␣ is a single trailing space).
- Copies the legitimate Windows System Assessment Tool executable, winsat.exe, and the Windows Multimedia API DLL, winmm.dll, to %TEMP%\<directory>\system32.

- Patches the legitimate DLL file, %TEMP%\<directory>\system32\winmm.dll , by replacing the entry point with malicious code that executes WastedLocker from the configured ADS path.
- Launches the legitimate executable, %TEMP%\<directory>\system32\winsat.exe , which in turn executes WastedLocker with administrative privileges without alerting the victim via a UAC prompt.

EXECUTION OPTIONS/PARAMETERS

To determine the action of WastedLocker when executed, options and parameters can be passed to define how it will operate

- -r - Seemingly the initial or default execution option, as used with the malware hidden within an ADS of a legitimate file, for example %APPDATA%\\<filename>:bin -r.
  - Delete volume shadow copies using the Volume Shadow Service Admin Tool vssadmin.exe Delete Shadows /All /Quiet to disrupt system restoration.
  - Copy the ransomware executable to %WINDIR%\\System32\\ using a random filename from the generation method.
  - Take ownership of this copied file using the take ownership utility takeown.exe /F %WINDIR%\\System32\\<filename>.exe.
  - Create and start a new service using a random name from the generation method, appending Ms if this clashes with an existing service name, with the 'Path to Executable' value set to %WINDIR%\\System32\\<filename>.exe -s.
  - Once the process has finished, the created service is stopped and then deleted, potentially using the Windows command line interface, cmd.exe, along with choice.exe to automatically and silently respond to any interactive prompts. As such, any endpoint executing the command cmd.exe (choice.exe), especially when followed by the del command and %APPDATA%\\<filename> path is potentially indicative of the WastedLocker service removal process.
- -s - Started as a service, commences the encryption phase.
- -p <directory> - Priority encryption of a specified directory or path, normal encryption continues once this is complete.
- -f <directory> - Seemingly a 'force' parameter that only encrypts the specified directory.

  In the case of the initial steps or service installation failing, changes to the system security zones are made within the registry key

HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\ZoneMap (Figure 4) to reportedly facilitate access to remote drives prior to the encryption process commencing:

- Automatic detection of an intranet enabled by setting the AutoDetect value to 1.
- Delete the intranet sites and proxy bypass options IntranetName and ProxyBypass.
- Disable UNC paths from being mapped to the local intranet security zone by setting the UNCAsIntranet value to 0.

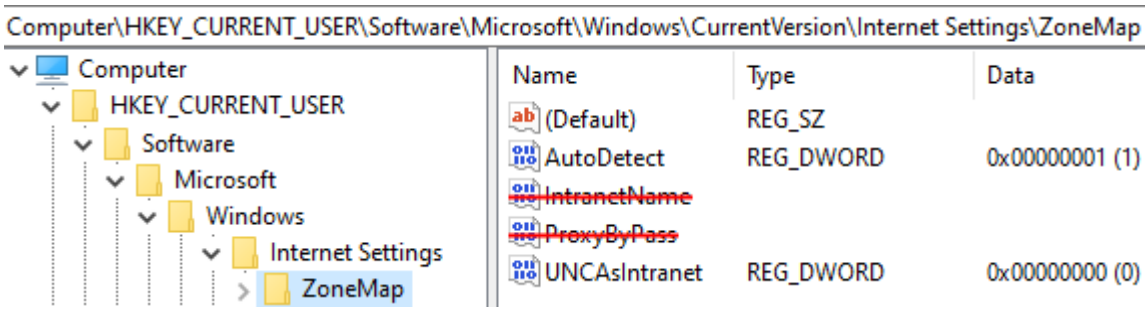

Figure 4 - Remote drive access registry changes

DEFENSE EVASION

To avoid detection and thwart recovery attempts, it is understood that WastedLocker can employ techniques to delete local backups as well as disabling end-point security solutions.

Whilst these capabilities may change depending on the victim organization's configuration, the following have been observed across campaigns:

- Deletion of Volume Shadow Copies, typically achieved using one or both native Windows commands:
  - Volume Shadow Copy Service administrative command-line tool: vssadmin.exe delete shadows /all /quiet.
  - Windows Management Instrumentation command-line utility: wmic.exe shadowcopy delete /nointeractive
- Reconfiguration of Windows Defender to disable behavioral monitoring and membership of the Microsoft Active Protection Service (MAPS) along with excluding rundll32.exe and DLL files from both real-time and scheduled scanning: %SYSTEM32%\WindowsPowershell\v1.0\powershell.exe Set-MpPreference -DisableBehaviorMonitoring $true; Set-MpPreference -MAPSReporting 0 ; Set MpPreference -ExclusionProcess rundll32.exe; Set-MpPreference -ExclusionExtension dll

- Reconfiguration of the Windows Firewall to permit outbound network access from the rundll32.exe process via any protocol: %SYSTEM32%\netsh.exe advfirewall firewall add rule name="Rundll32" dir=out action=allow protocol=any program="%SYSTEM32%\rundll32.exe".

ENCRYPTION

As is to be expected with any notable ransomware threat, WastedLocker attempts to encrypt data on local fixed and removable storage as well as shared or remote volumes. Whilst many threats make use of a targeted file extension list, typically including productivity files and excluding system files, WastedLocker only makes use of an exclude list to prevent critical directories and file extensions from being encrypted (Figures 5 and 6).

%APPDATA%

%PROGRAMDATA%

%PROGRAMFILES%

%PROGRAMFILES(X86)%

%TEMP%

%WINDIR%

\$recycle.bin

\appdata

\bin

\boot

\bootmgr

\caches

\dev

\etc

\grldr

\initdr

\lib

\ntldr

\run

\sbin

\sys

\system volume information

\users\all users

\var

\vmlinuz

\webcache

\windowsapps

c:\recovery

Figure 5 - Directories excluded from the encryption process

386, adv, ani, bak, bat, bin, cab, cmd, com, cpl, cur, dat, diagcab, diagcfg, dll, drv, exe, hlp, hta, icl, icns, ics, idx, ini, key, lnk, mod, msc, msi, msp, msstyles, msu, nls, nomedia, ocx, ps1, rom, rtp, scr, sdi, shs, sys, theme, themepack, wim, wpx

Figure 6 - File extensions excluded from the encryption process

Additionally, presumably for speed and effectiveness, files smaller than ten bytes are ignored whilst large files, sometimes ignored by other threats, are encrypted in 64MB blocks.

To further evade detection, and potentially thwart end-point security solutions that employ behavioral analysis of file operations, WastedLocker makes use of memory-mapped file (MMF) access to encrypt files in memory, negating the need for multiple disk input/output (IO) operations that would appear suspicious.

This method places a cached copy of a file in memory where it can be encrypted before being closed and written back to disk by the Windows Cache Manager. This native process reduces the number of disk IO operations using 'lazy writing' that 'flushes the cache' at intervals determined by the operating system and effectively performs multiple file operations at once. As such, the number of these otherwise highly suspicious disk operations are reduced as well as being performed by a valid system context that, to all intents and purposes, will appear legitimate.

Utilizing the same encryption method as later variants of BitPaymer, files encrypted by WastedLocker use Advanced Encryption Standard (AES), with a unique 256-bit key and 128-bit initialization vector (IV), in Cipher Block Chaining (CBC) mode. The use of CBC ensures that as each unencrypted block is processed, it is combined with the cipher text of the previous block using a bitwise XOR operation and thus ensures that identical blocks of unencrypted data do not appear alike in the final encrypted output.

Subsequently, the key and IV, along with an MD5 cryptographic hash of the original file, are encrypted using an embedded 4096-bit public RSA key before being base64 encoded and saved in a ransom note for that file. The presence of an MD5 hash for each file suggests that the decryption routine has some form of validation although this is likely only for 'reporting' purposes as there would be no way of recovering a file that fails the decryption process.

As noted by Kaspersky, the use of a fixed RSA public key in this process could be considered a weakness if the ransomware were to be widely distributed. Unfortunately, given that each WastedLocker campaign is customized for the target organization, this flaw is somewhat eliminated, and the use of a robust encryption method will make the process likely irreversible without obtaining the decryption keys.

In keeping with the threat name, once a file has been encrypted the tell-tale file extension is appended, <filename>.<extension>.<victim>wasted , in addition to the creation of a ransom note for each file as <filename>.<extension>.<victim>wasted_info.

RANSOM

Whilst the majority of ransomware threats typically place ransom notes in prominent locations, such as on the victim's desktop or within their documents folder, victims are unlikely to miss WastedLocker's ransom note due to the creation of one ransom note per encrypted file (Figure 7).

```
<VICTIM ORGANIZATION>

YOUR NETWORK IS ENCRYPTED NOW

USE <EMAIL_ADDRESS> | <EMAIL_ADDRESS> TO GET THE PRICE FOR YOUR DATA

DO NOT GIVE THIS EMAIL TO 3RD PARTIES

DO NOT RENAME OR MOVE THE FILE

THE FILE IS ENCRYPTED WITH THE FOLLOWING KEY:
[begin_key]<BASE64_KEY>[end_key]
KEEP IT
```

Figure 7 - Example Ransom Note

In addition to the base64 encoded block, containing the key, IV and a MD5 cryptographic hash of the original file, contact email addresses are provided so that the victim can initiate 'negotiations'. These email addresses are typically five-digit numeric values, reportedly

random or unique to the victim, and make use of privacy-focused web-based email providers such as Protonmail and Tutanota.

As is expected with big game hunter ransomware campaigns, WastedLocker ransom demands have reportedly ranged from USD 0.5 to 10 million and have been demanded as paid using the Bitcoin cryptocurrency.

RECOMMENDATIONS

EMPLOYEE SECURITY AWARENESS

Whilst the use of compromised websites may be difficult for the average user to identify, security awareness training remains an important step in ensuring that those on the front line are able to spot and stop many common attack vectors. Given the current global situation, with many working from home and adapting to increased online habits, employees should be reminded to be suspicious of any unsolicited or unusual communication, especially those containing attachments or links, as well as being mindful of any websites they visit using corporate assets.

PRACTICE LEAST PRIVILEGE

To limit the impact of any credential compromise, the enforcement of least privilege policies can prevent day-to-day accounts being compromised and used to gain elevated access to other systems. As such, organizations should ensure that devices, services and users only have the privileges required to perform their function, effectively segregating and limiting access.

MONITORING

Through the continuous monitoring of endpoint security events, organizations can maintain visibility of their environments and identify suspicious activity before it becomes a problem. Activity such as unexpected connections between hosts may provide an early indication of lateral movement whilst end-point behaviors such as the execution of administrative tools by standard users could be indicative of a malicious process being installed or executed.

PATCH MANAGEMENT

Tried and tested techniques continue to be employed by threat actors including the exploitation of common vulnerabilities in exposed systems and end-point applications. As

such, organizations should ensure that the 'low-hanging fruit' are secured, such as ensuring internet-facing infrastructure is regularly updated and patched, whilst having robust plans in place to replace any systems using end-of-life operating systems or software.

When applying updates or patches, these should only be obtained from verified legitimate sources, such as the original vendor, and not third-party sources. Additionally, where possible, the validity of any patch should be checked against published checksums or digital signatures prior to execution or application.

SECURE SENSITIVE DATA

Whilst those behind WastedLocker do not appear to be actively stealing data, consideration should be given to any legal or regulatory requirements for data storage to ensure that sensitive data is adequately encrypted and/or securely stored to prevent unauthorized access, be that internal or external in origin.

APPLICATION PERMIT/DENY LISTS

The use of application permit and deny lists can detect and prevent the execution of unauthorized or unknown executables, effectively hardening an operating system against attack. When used in environments that have limited change, such as on webservers, a baseline can be generated and any subsequent attempt to launch an executable file, be that from another location, or a modified file, can be denied.

Furthermore, denying the execution of administrative tools by standard user accounts can prevent their misuse by threat actors. Tools abused by WastedLocker include the Windows Command Line, script interpreters, such as the Windows Scripting Host and PowerShell, in addition to utilities that disable security settings and remove backup files such as the 'Volume Shadow Service Admin Tool' and the 'Windows Management Instrumentation command-line utility'.

DISASTER RECOVERY PLANNING

As with all ransomware attacks, it is imperative that organizations have procedures in place to regularly backup and verify the integrity of their data, as well as performing periodic exercises to ensure that disaster recovery plans work in practice. Additionally, given that many attacks move laterally across networks, backups should not be solely stored on an 'online' system; both offline and offsite storage, if regularly updated, can facilitate the restoration of services in the event of a large-scale catastrophic incident, potentially even allowing restoration to a 'stand-by' site that can provide business continuity.

NETWORK SEGREGATION

The use of appropriate network segregation, often by creating separate logical segments for assets that share a similar risk profile and limiting communications, especially between end-points, allows attacks to be contained and provides damage limitation, potentially preventing threats from propagating further across an organization.

INDICATORS OF COMPROMISE

Given that each WastedLocker ransomware threat is custom built for the specific victim, common indicators of compromise (IOC) such as file hashes provide no actionable intelligence and should not be relied upon to counter this threat.

POTENTIAL C2 DOMAINS

Reports indicate that consistent command and control (C2) domains have been used by the group, likely in the initial compromise phase, when CobaltStrike is deployed. As such, the following domains may be indicative of Evil Corp/WastedLocker activity:

- adsmarketart.com
- advancedanalysis.be
- advertstv.com
- amazingdonutco.com
- cofeedback.com
- consultane.com
- dns.proactiveads.be
- mwebsoft.com
- rostraffic.com
- traffichi.com
- typiconsult.com
- websitelistbuilder.com

POTENTIALLY SUSPICIOUS BEHAVIOURS

Identification of the following behaviors, grouped by tactic, could be indicative of malicious activity consistent with WastedLocker or a similar threat:

Execution

- Monitor for, and/or deny, the unexpected execution of scripts from the %TEMP% directory using wscript.exe as used by SocGholish.
- Monitor for, and/or deny, the unexpected execution of PowerShell scripts, especially by non-administrative users, as used by CobaltStrike and to reconfigure Windows Defender.

Privilege Escalation

- Monitor for, and/or deny, the unexpected execution of the take ownership utility takeown.exe /F, especially by non-administrative users.
- Monitor for the creation of a mount point named C:\Windows␣ (where ␣ is a single trailing space).
- Monitor for the creation of a system32 directory anywhere within the %TEMP% directory.
- Monitor for, and/or deny, the unexpected execution of any executable file from the %TEMP% directory.
- Monitor for, and/or deny, the unexpected execution of the Windows System Assessment Tool winsat.exe.

Defense Evasion

- Monitor for, and/or deny, the unexpected execution of the Volume Shadow Service Admin Tool vssadmin.exe.
- Monitor for, and/or deny, the unexpected execution of the Windows Management Instrumentation command-line utility wmic.exe.
- Monitor for, and/or deny, the unexpected execution of the command-line interface cmd.exe in addition to the use of the choice.exe automation utility

- Monitor for, and/or deny, the unexpected modification of the system security zones within the Windows Registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap.
- Monitor for, and/or deny, the unexpected execution of the network shell utility netsh.exe as used to reconfigure the Windows Firewall.

MITRE ATT&CK

Technique	Tactic
T1005 - Data from Local System	Collection
T1059.001 - Command and Scripting Interpreter: PowerShell	Execution
T1059.003 - Command and Scripting Interpreter: Windows Command Shell	Execution
T1059.007 - Command and Scripting Interpreter: JavaScript/JScript	Execution
T1071.001 - Application Layer Protocol: Web Protocols	Command And Control
T1083 - File and Directory Discovery	Discovery
T1106 - Native API	Execution
T1189 - Drive-by Compromise	Initial Access
T1222.001 - File and Directory Permissions Modification: Windows File and Directory Permissions Modification	Defense Evasion
T1486 - Data Encrypted for Impact	Impact
T1490 - Inhibit System Recovery	Impact
T1543.003 - File and Directory Permissions Modification: Create or Modify System Process: Windows Service	Persistence Privilege Escalation
T1548.002 - Abuse Elevation Control Mechanism: Bypass User Access Control	Defense Evasion Privilege Escalation
T1562.001 - Impair Defenses: Disable or Modify Tools	Defense Evasion
T1562.004 - Impair Defenses: Disable or Modify System Firewall	Defense Evasion
T1564.004 - Hide Artifacts: NTFS File Attributes	Defense Evasion
T1569.002 - System Services: Service Execution	Execution

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +1-929-399-8495
Panama City