Acronis
Global Cyber Summit 2020

Acronis Cyber Protection Operation Center

Evolution in Malware Tactics and Techniques

#CyberFit

SINGAPORE

Evolution of Attack Tactics and Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Email Collection (3)	Non-Standard Port		Resource Hijacking
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling		Service Stop
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)		System Shutdown/Reboot
		Pre-OS Boot (3)		Indirect Command Execution	Unsecured Credentials (6)	Process Discovery		Man-in-the-Middle (1)	Remote Access Software		
		Scheduled Task/Job (5)		Masquerading (6)		Query Registry		Screen Capture	Traffic Signaling (1)		
		Server Software Component (3)		Modify Authentication Process (3)		Remote System Discovery		Video Capture	Web Service (3)		
		Traffic Signaling (1)		Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
				Modify Registry		System Information Discovery					
				Obfuscated Files or Information (5)		System Network Configuration Discovery					
				Pre-OS Boot (3)		System Network Connections Discovery					

MITRE | ATT&CK®

Acronis
Global Cyber Summit 2020

Evasion Techniques

#CyberFit

Ragnar locker Ransomware

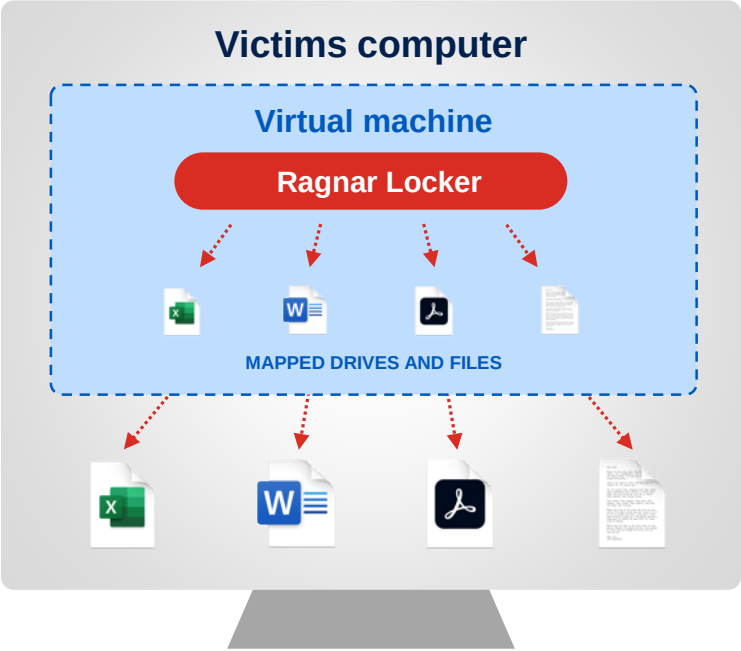
Install a virtual machine and conceal the ransomware within

Infection process:

1) Microsoft Installer downloads and executes MSI e.g. with GPO
2) Installs Oracle VirtualBox with a Windows XP virtual machine
3) Attempts to terminate anti-virus process and services
   - Taskkill /IM <process_name> /F
   - sc stop <service_name>
4) Maps all available drives inside the virtual machine
5) Encrypt data through the trusted **VboxHeadless.exe** app

Bypasses most anti-ransomware solutions

Maze group adapted this technique in September 2020



Ragnar Locker. Preparing the Virtual Machine

Script deletes the local shadow copies

```
vssadmin delete shadows /all /quiet
```

Mapping all drives as writeable in the VBox config file

```
Set driveid=0
FOR %%d IN (C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO (
      IF EXIST %%d:\ (
            Set /a driveid+=1
            echo ^<SharedFolder name=”!driveid!” hostPath=”%%d:\” writable=”true”/^> >>sf.txt
         )
```

Install.bat starts the virtual machine

```
“%binpath%\VboxHeadless.exe” –startvm micro -v off
```

RIPlace Evasion Technique

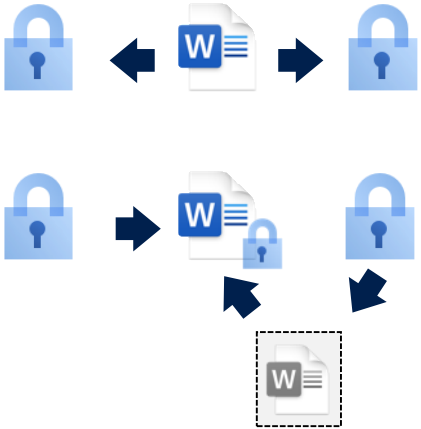
Use old symlink + file rename function to bypass monitoring solutions

Common Ransomware

Read target file to memory
Writing encrypted data into new file

Rename new file and overwrite target File with `FileRenameInformation`

Security solution can see the rename and may **prevent the write** operation



RIPlace technique

Read target file to memory
Writing encrypted data into new file

Create a **symlink** for the target file with `DefineDosDevice` API

Rename target file through symlink `FltGetDestinationFileNameInformation`
Fails to get correct destination path

Security solution **does not see the rename**
File is overwritten with encrypted content

Bypasses most AV & EDR solutions

Robin Hood Ransomware uses Vulnerable Driver

Using Gigabyte driver exploit to disable security products

Infection process:

1. Install **legitimate** Gigabyte **kernel driver** GDRV.SYS.
2. Exploit a **known vulnerability** in it to disable Windows kernel protection
3. Load own malicious unsigned kernel driver and **disable anti-virus**
4. **Encrypt files** with Robin Hood ransomware without interference

Self-Defense of security software is important

Snatch ransomware achieves the same by rebooting Windows into safe-mode

Ransomware Tactics Change

Not only the techniques have evolved, but also the tactics

Steal Data

- Steal data = data breach ➔ fine
- 700+ companies already had their data leaked. Cases with 10 TB+
- Maze 260+, Conti/Ryuk 100+, Sodinokibi 90+, DoppelPaymer 60+
- US OFAC regulation on payments

DDoS Attacks

- DDoS attacks as an additional **means of pressure** against the victim
- DDoS attacks **as smokescreens** to distract the IT department

IoT + Cloud

- Ransomware attacks **on cloud services** such as DBs and Kubernetes container
- Ransomware on **OT** & **IoT devices** such as ICS, but also smart TVs and coffee makers

Acronis
Global Cyber Summit 2020

MacOS

#CyberFit

Mac Malware is Increasing

Shlayer (August)

- Malware disguised as Flash player, downloading Adware
- Apples malware check bypassed ➔ malware notarized & signed
- Bypasses macOS Gatekeeper security

XCSSET (August)

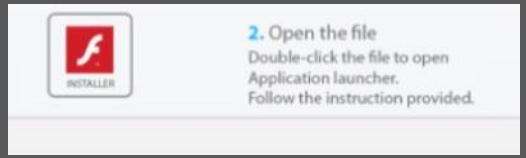
- **Injects into Xcode** developer projects ➔ supply chain risk
- **2 vulnerabilities** for Safari to steal passwords from any web site
- Steal data from other apps: Evernote, Notes, Skype, Telegram, …

ThiefQuest ransomware (July)

- Mach-O **file infection** opening up a backdoor
- Ransomware claiming AES-256, in reality weak RC2 encryption
- They ask for $50 ransom + no user ID ➔ profit is not the only goal

Normally, Chrome blocks the Installation of the new plugins. Proceed as follows:

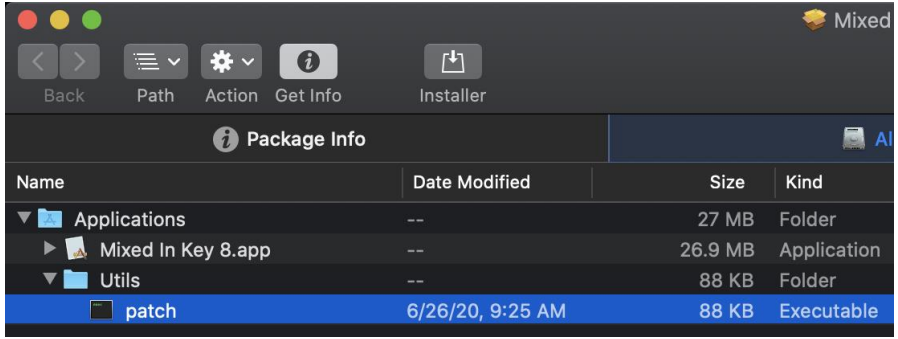
1. Click on “Show in Folder”.



2. Open the file and follow the instruction.

* This message will no longer appear after this installation.

ThiefQuest Ransomware & Backdoor




```
#!/bin/sh
mkdir /Library/mixednkey

mv /Applications/Utils/patch /Library/mixednkey/toolroomd
rmdir /Application/Utils

chmod +x /Library/mixednkey/toolroomd

/Library/mixednkey/toolroomd &
```

Patrick Wardle

Acronis
Global Cyber Summit 2020

Phishing

#CyberFit

Phishing is Increasing on Several Fronts

Phishing attacks going after 2FA

- Asking employee to enter 2FA codes into phishing page
- Exfiltrate through api.telegram.org/bot & automatically login

Protecting phishing site with a CAPTCHA

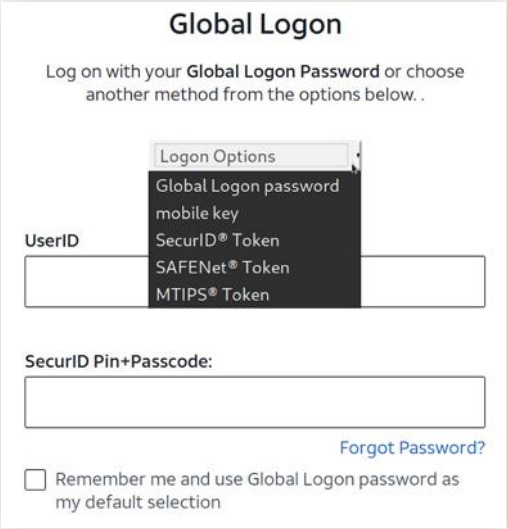
- Has to be solved before redirecting to phishing site

Hosting phishing page on trusted public cloud domain

- e.g. Microsoft Azure, Microsoft Dynamics, IBM Cloud
- In Q3, 8% of the clients had a URL blocked – 51% were HTTPS

Phishing is often the start of further attacks

Phishing site for employees



sucuri.net

Summary

Attacks are evolving ➔ comprehensive integrated protection approach is needed

Defense Evasion

- Hiding in virtual machines
- RIPlace monitoring bypass
- Vulnerable system drivers

Acronis Cyber Protect

- Threat agnostic detection
- Behavior based detection
- Knowledge of low-level file I/O

Not just Windows

- Notarized malware on MacOS
- Infect local XCode projects
- Ransomware on cloud servers e.g. ElasticSearch & MongoDB

Acronis Cyber Protect

- Cyber Protection on macOS
- Cyber Protection on Linux
- URL filtering

Phishing Increased

- Phishing against 2FA codes for abuse in real-time
- Abuse of public cloud trust
- Obstruction with CAPTCHAs

Acronis Cyber Protect

- URL filtering
- Web category based filtering
- Behavior based detection

Acronis
Cyber Foundation

Building a more knowledgeable future

#CyberFit

CREATE, SPREAD AND PROTECT KNOWLEDGE WITH US!

www.acronis.org

Building new schools • Providing educational programs • Publishing books