STEVEN H.

RANSOM-WARE

Internal analysis

Start Now →

RANSOMWARE

https://www.nomoreransom.org/en/decryption-tools.html

INTRODUCTION TO RANSOMWARE

Definition of ransomware

Ransomware is a type of malicious software (malware) designed to block access to a computer system or data until a sum of money, or ransom, is paid. It typically encrypts the victim's files or locks their screen, rendering the system or files inaccessible. Ransomware attacks often demand payment in cryptocurrency to make tracing the perpetrators difficult.

MALWARE

https://attack.mitre.org/software/

MALWARE EXAMPLES

Ransomware

BlackCat – also known as “ALPHV”- is a ransomware which uses ransomware-as-a-service model and double ransom schema (encrypted files and stolen file disclosure).

Information Stealer

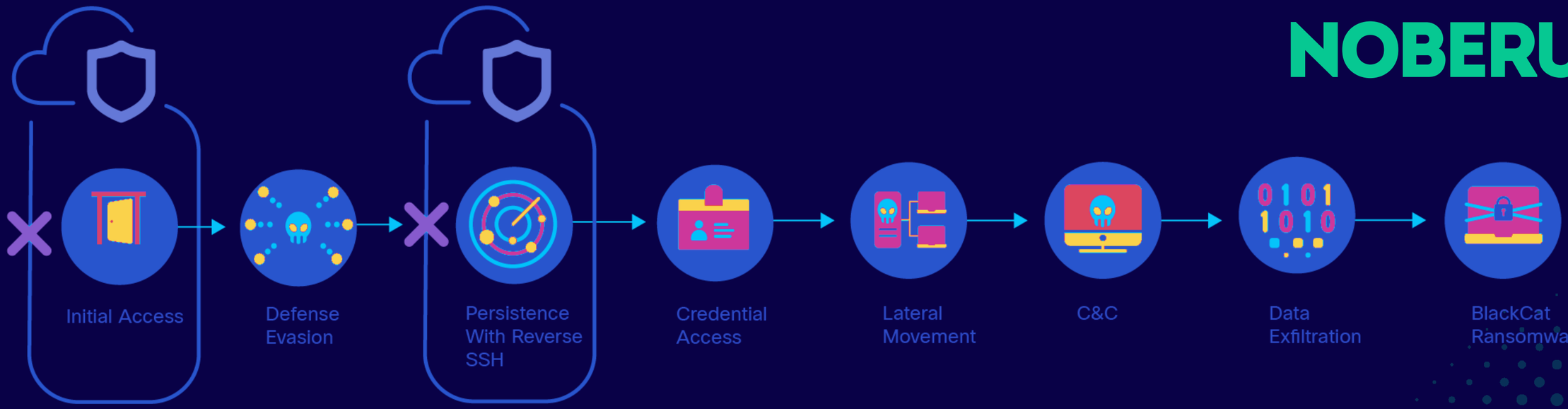
ZingoStealer is an information stealer released by a threat actor known as “Haskers Gang.” The malware leverages Telegram chat features to facilitate malware executable build delivery and data exfiltration

Loaders

BumbleBee is a loader that has anti-virtualization checks and loader capabilities. The goal of the malware is to take a foothold in the compromised system to download and execute additional payloads.

RANSOMWARE

BLACKCAT / ALPHV / NOBERUS

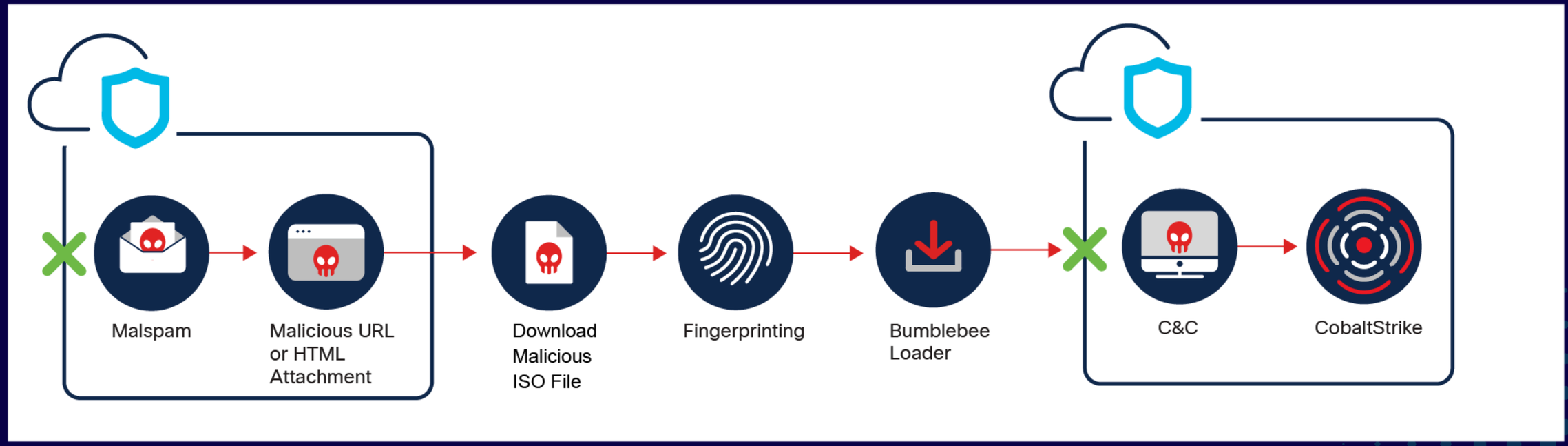


INFORMATION STEALERS

ZINGOSTEALER

LOADERS

BUMBLEBEE



INITIAL ACCESS & LOADER

DEEP DIVES

Rubeus

Rubeus is a C# toolset for raw Kerberos interaction and abuses.

FUD-Loader

Malware tool designed to deliver and execute malware on a system while evading detection by security software such as antivirus programs and intrusion detection systems.

INFOSTEALER & COMMAND/CONTROL (C2)

DEEP DIVES

SapphireStealer

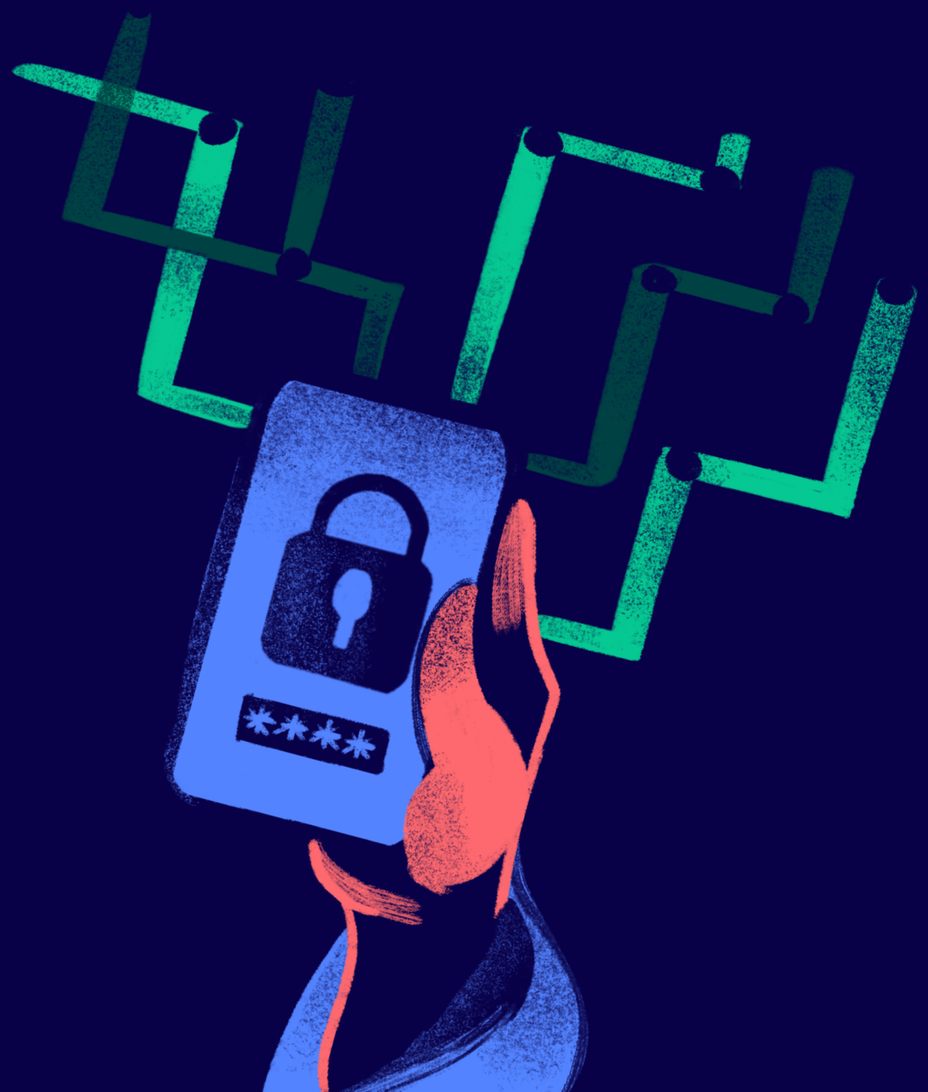
A simple stealer with sending logs to your EMAIL

Covenant

Covenant is a .NET C2 framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative platform for red teamers.

DEMO

https://github.com/GhostPack/Rubeus



RUBEUS

Rubeus can:

- Gather information about domain trusts.
- Forge a ticket-granting (golden) ticket.
- Create silver tickets.
- Kerberoast service tickets.
- Rubeus can reveal the credentials of accounts that have Kerberos pre-authentication disabled.

DEMO

https://github.com/cobbr/Covenant

COVENANT

Covenant can:

- **C2 Infrastructure:** Establishes and manages command and control for penetration testing.
- **Multi-Platform Support**: Compatible with Windows, macOS, and Linux.
- **Grunt Management**: Executes and controls commands on compromised systems.
- **Modular and Extensible**: Supports custom modules and payloads.
- **Secure Communication**: Uses HTTPS and encryption for secure data transmission.

DEMO

https://github.com/0day2

FUD-LOADER & SAPHIRESTEALER

Fully Undetecatable Loader

- Use of silent process execution

SaphireStealer

- Steals browser creds, database, specific files
- Exfiltrates using email or Telegram.

STEVEN H.

Ransomware Presentation

THANK YOU FOR ATTENTION

See You Next →