

NETMANAGEIT

Intelligence Report

Phorpiex Malware Campaign

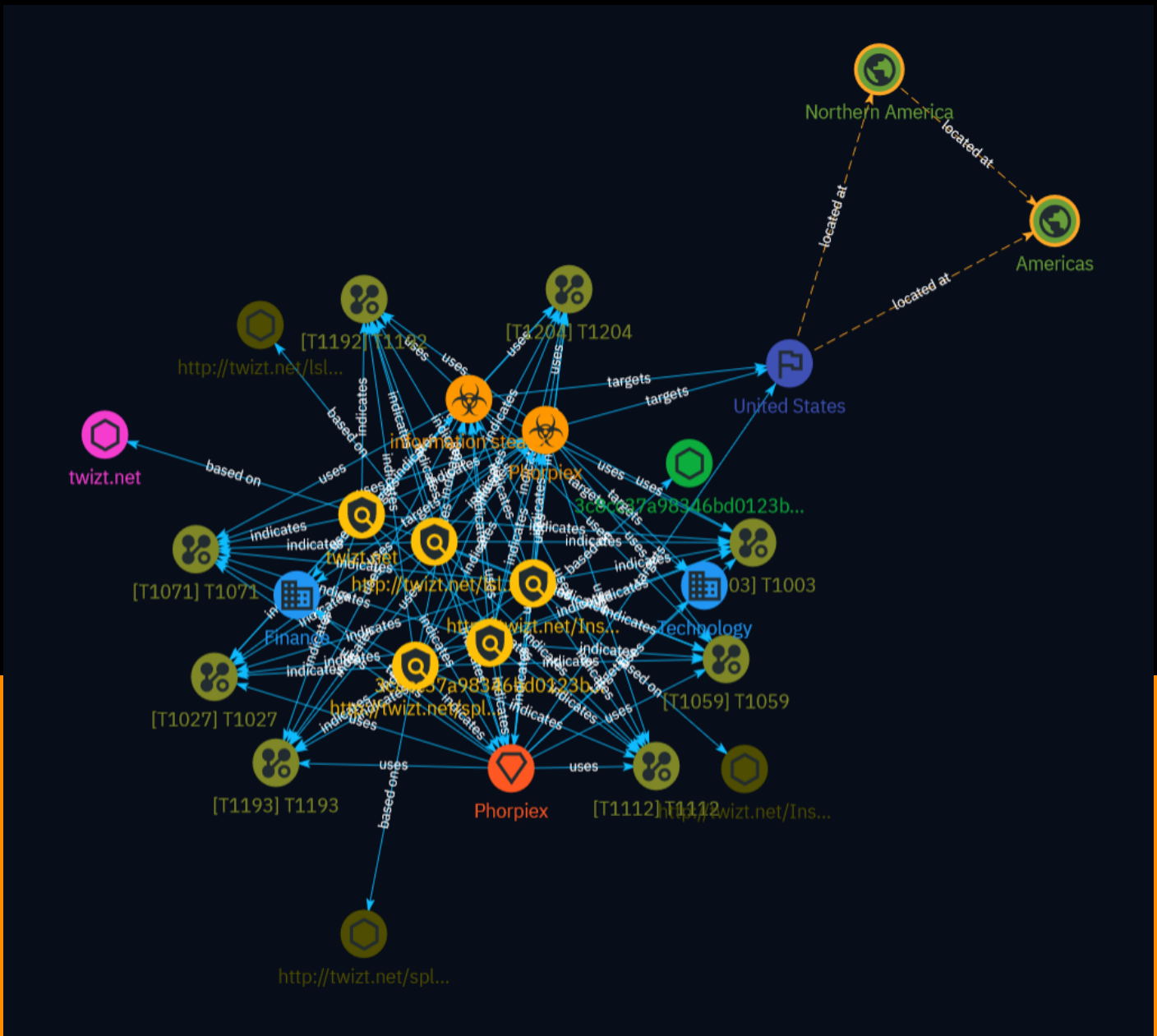


Table of contents

Overview

● Description	4
● Confidence	4
● Content	5

Entities

● Indicator	6
● Malware	9
● Intrusion-Set	10
● Attack-Pattern	11
● Country	16
● Region	17
● Sector	18

Observables

● Url	19
● StixFile	20
● Domain-Name	21

External References

● External References	22
-----------------------	----

Overview

Description

This report provides analysis of a malware campaign distributing the Phorpiex information stealer malware. The attackers use shortcut files containing malicious macros to infect victims and download additional payloads. The campaign targets entities in the technology and finance sectors across Europe and North America.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

http://twizt.net/spl.exe

Description

Threat: malware_download - Reporter: cocaman - Status: online

Pattern Type

stix

Pattern

[url:value = 'http://twizt.net/spl.exe']

Name

http://twizt.net/lslut.exe

Description

Threat: malware_download - Reporter: abuse_ch - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://twizt.net/lslut.exe']

Name

http://twizt.net/Installed

Description

Threat: malware_download - Reporter: abuse_ch - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://twizt.net/Installed']

Name

3c8cc37a98346bd0123b35e5ccd87bd07d69914dae04f8b49f61c150d96e9d1f

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'3c8cc37a98346bd0123b35e5ccd87bd07d69914dae04f8b49f61c150d96e9d1f']

Name

twizt.net

Pattern Type

stix

Pattern

[domain-name:value = 'twizt.net']

Malware

Name

Phorpiex

Name

information stealer

Intrusion-Set

Name

Phorpiex

Attack-Pattern

Name

T1193

ID

T1193

Name

T1192

ID

T1192

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer

systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](<https://attack.mitre.org/techniques/T1059/004>) while Windows installations include the [Windows Command Shell](<https://attack.mitre.org/techniques/T1059/003>) and [PowerShell](<https://attack.mitre.org/techniques/T1059/001>). There are also cross-platform interpreters such as [Python](<https://attack.mitre.org/techniques/T1059/006>), as well as those commonly associated with client applications such as [JavaScript](<https://attack.mitre.org/techniques/T1059/007>) and [Visual Basic](<https://attack.mitre.org/techniques/T1059/005>). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](<https://attack.mitre.org/tactics/TA0001>) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](<https://attack.mitre.org/techniques/T1021>) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1027

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](<https://attack.mitre.org/techniques/T1140>) for [User Execution](<https://attack.mitre.org/techniques/T1204>). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly

benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](<https://attack.mitre.org/techniques/T1027/010>) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](<https://attack.mitre.org/techniques/T1059>). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](<https://attack.mitre.org/techniques/T1566>). While [User Execution](<https://attack.mitre.org/techniques/T1204>) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](<https://attack.mitre.org/techniques/T1534>). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](<https://attack.mitre.org/techniques/T1219>), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](<https://attack.mitre.org/techniques/T1204>). For example, tech support scams can be facilitated through [Phishing](<https://attack.mitre.org/techniques/T1566>), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](<https://attack.mitre.org/techniques/T1219>).(Citation: Telephone Attack Delivery)

Name

T1112

ID

T1112

Description

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](<https://attack.mitre.org/software/S0075>) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](<https://attack.mitre.org/software/S0075>) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](<https://attack.mitre.org/techniques/T1078>) are required, along with access to the remote system's [SMB/Windows Admin Shares](<https://attack.mitre.org/techniques/T1021/002>) for RPC communication.

Name

T1071

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

T1003

ID

T1003

Description

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](<https://attack.mitre.org/tactics/TA0008>) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

Country

Name

United States

Region

Name

Northern America

Name

Americas

Sector

Name

Technology

Description

Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Name

Finance

Description

Public and private entities involved in the allocation of assets and liabilities over space and time.

Url

Value

<http://twizt.net/spl.exe>

<http://twizt.net/lslut.exe>

<http://twizt.net/Installed>

StixFile

Value

3c8cc37a98346bd0123b35e5ccd87bd07d69914dae04f8b49f61c150d96e9d1f

Domain-Name

Value

twizt.net

External References

-
- <https://otx.alienvault.com/pulse/6606bdf87ea4eede65ff4d0c>