Mar 19 2024

NETMANAGEIT

Intelligence Report

RisePro stealer targets Github users in campaign

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new campaign called gitgub is distributing the RisePro information stealer through malicious GitHub repositories. The campaign has already exfiltrated over 700 stolen data archives to Telegram channels. RisePro uses obfuscation techniques like import hashing and virtualization to evade detection.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

digitalxnetwork.com

Pattern Type

stix

Pattern

[domain-name:value = 'digitalxnetwork.com']

Name

https://digitalxnetwork.com/INSTALLER%20PA$$WORD%20GIT1HUB1FREE.rar

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1706375961, 'iso': '2024-01-27T12:19:21-05:00'} - **IPQS: Domain:** digitalxnetwork.com - **IPQS: IP Address:** 144.76.3.10

Pattern Type

stix

Pattern

[url:value = 'https://digitalxnetwork.com/INSTALLER%20PA$$WORD%20GIT1HUB1FREE.rar']

Name

f52ba7d8a820d32c502c4aaef4bf9690fc0ca97b97c683b43057d82c06294257

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f52ba7d8a820d32c502c4aaef4bf9690fc0ca97b97c683b43057d82c06294257']

Name

b0e194ed54bafa753bda5761c1264b67a5c438ee7a9ed624a83be913f037dcbb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b0e194ed54bafa753bda5761c1264b67a5c438ee7a9ed624a83be913f037dcbb']

Name

492a71bf56d2e89d0b9c5d70ed6c37acea89c8134fa5ba623bce74b3f0fb189e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '492a71bf56d2e89d0b9c5d70ed6c37acea89c8134fa5ba623bce74b3f0fb189e']

Name

0ff1e4724b5b02a034789e328531f04a660fd1bade2ad9e73c8b748e5f3e0753

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0ff1e4724b5b02a034789e328531f04a660fd1bade2ad9e73c8b748e5f3e0753']

Name

059067376a6271fdead553b471ec899dec3662ec09bd5c3833911c87ea062e92

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '059067376a6271fdead553b471ec899dec3662ec09bd5c3833911c87ea062e92']

Name

193.233.132.32

Description

- **Zip Code:** N/A - **ISP:** Chromis It - **ASN:** 216319 - **Organization:** Chromis It - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 193.233.132.32 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Florida - **City:** Jacksonville - **Latitude:** 30.33213425 - **Longitude:** -81.65567017

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.233.132.32']

Name

176.113.115.227

Description

ISP: Cat Technologies Co. Limited **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **2052:** ``` HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Sat, 30 Dec 2023 21:08:27 GMT Content-Type: text/html; charset=utf-8 Content-Length: 179 Connection: keep-alive ``` ---------- **3352:** ``` HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Tue, 26 Dec 2023 06:16:12 GMT Content-Type: text/html; charset=utf-8 Content-Length: 179 Connection: keep-alive ``` ---------- **8090:** ``` HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Sun, 31 Dec 2023 20:13:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 179 Connection: keep-alive ``` ---------- **9212:** ``` HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Tue, 19 Dec 2023 05:32:58 GMT Content-Type: text/html; charset=utf-8 Content-Length: 179 Connection: keep-alive ``` ----------

Pattern Type
stix
Pattern
[ipv4-addr:value = '176.113.115.227']

Malware

Name
RisePro

Name
information stealer

Intrusion-Set

Name
RisePro

Attack-Pattern

Name
T1056
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name
T1070
ID
T1070
Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

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

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

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1140

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

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.

Domain-Name

Value
digitalxnetwork.com

Url

Value
https://digitalxnetwork.com/INSTALLER%20PA$$WORD%20GIT1HUB1FREE.rar

StixFile

Value
f52ba7d8a820d32c502c4aaef4bf9690fc0ca97b97c683b43057d82c06294257
b0e194ed54bafa753bda5761c1264b67a5c438ee7a9ed624a83be913f037dcbb
492a71bf56d2e89d0b9c5d70ed6c37acea89c8134fa5ba623bce74b3f0fb189e
0ff1e4724b5b02a034789e328531f04a660fd1bade2ad9e73c8b748e5f3e0753
059067376a6271fdead553b471ec899dec3662ec09bd5c3833911c87ea062e92

IPv4-Addr

Value
193.233.132.32
176.113.115.227

External References

- https://www.gdatasoftware.com/blog/2024/03/37885-risepro-stealer-campaign-github
- https://otx.alienvault.com/pulse/65f41fc80e535711927f9db2