Jul 24 2023

NETMANAGEIT

Intelligence Report

HotRat: The Risks of Illegal Software Downloads and Hidden AutoHotkey Script Within

fon1.sells-it.net
srxy123.is-a-geek.co...
51-83-136-132.xyz
27.1.0.189
[T1104] Multi-Stage Channels
[T1055] Process Injection
16.1.0.106
[T1566] Phishing
185.205.209.206
13.70.2.40
[T1036] Masquerading
HotRat
Akira
dynsys.is-a-guru.com
samaerx.ddnsfree.com
AsyncRAT
foxn1.sells-it.net
[T1562] Impair Defenses
s1-filecr.xyz
[T1127] Trusted Developer...
14.1.9.124
[T1027] Obfuscated Files or...
foxn1.sells-it.net
[T1053] Scheduled Task/Job
[T1115] Clipboard Data
1.94.147.103
websites.theworkpc.c...
rec.casacam.net
s1-filecr.xyz

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The latest analysis shows that illegal software can be used to spread malware, including a variant of AsyncRAT, which can infect a victim’s computer and steal login credentials.

Confidence

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

15 / 100

Indicator

Name

27.1.0.189

Description

CC=KR ASN=AS9943 KangNam CableTV

Pattern Type

stix

Pattern

[ipv4-addr:value = '27.1.0.189']

Name

108.143.240.80

Description

CC=NL ASN=AS8075 MICROSOFT-CORP-MSN-AS-BLOCK

Pattern Type

stix

Pattern

[ipv4-addr:value = '108.143.240.80']

Name

51-83-136-132.xyz

Pattern Type

stix

Pattern

[domain-name:value = '51-83-136-132.xyz']

Name

dynsys.is-a-guru.com

Pattern Type

stix

Pattern

[hostname:value = 'dynsys.is-a-guru.com']

Name

16.1.0.106

Description

CC=US ASN=AS19647 HPES

Pattern Type

stix

Pattern

[ipv4-addr:value = '16.1.0.106']

Name

14.1.9.124

Description

CC=JP ASN=AS10000 Nagasaki Cable Media Inc.

Pattern Type

stix

Pattern

[ipv4-addr:value = '14.1.9.124']

Name

rec.casacam.net

Pattern Type

stix

Pattern

[hostname:value = 'rec.casacam.net']

Name
fon1.sells-it.net

Pattern Type
stix

Pattern
[hostname:value = 'fon1.sells-it.net']

Name
1.94.147.103

Description
CC=CN

Pattern Type
stix

Pattern
[ipv4-addr:value = '1.94.147.103']

Name
foxn1.sells-it.net

Pattern Type
stix

Pattern

[hostname:value = 'foxn1.sells-it.net']

Name

13.70.2.40

Description

CC=HK ASN=AS8075 MICROSOFT-CORP-MSN-AS-BLOCK

Pattern Type

stix

Pattern

[ipv4-addr:value = '13.70.2.40']

Name

websites.theworkpc.com

Pattern Type

stix

Pattern

[hostname:value = 'websites.theworkpc.com']

Name

samaerx.ddnsfree.com

Pattern Type

stix

Pattern

[hostname:value = 'samaerx.ddnsfree.com']

Name

185.205.209.206

Description

CC=BG ASN=AS44901 Belcloud LTD

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.205.209.206']

Name

s1-filecr.xyz

Pattern Type

stix

Pattern

[domain-name:value = 's1-filecr.xyz']

Name
srxy123.is-a-geek.com
Pattern Type
stix
Pattern
[hostname:value = 'srxy123.is-a-geek.com']

Malware

Name
HotRat

Name
Akira

Name
AsyncRAT

Attack-Pattern

Name

Trusted Developer Utilities Proxy Execution

ID

T1127

Description

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

Name

Masquerading

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)

Name

Process Injection

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

Scheduled Task/Job

ID

T1053

Description
Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name
Phishing

ID
T1566

Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security

tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Impair Defenses

ID

T1562

Description

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

Name

Obfuscated Files or Information

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

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

Clipboard Data

ID

T1115

Description

Adversaries may collect data stored in the clipboard from users copying information within or between applications. For example, on Windows adversaries can access clipboard data by using `clip.exe` or `Get-Clipboard`.(Citation: MSDN Clipboard)(Citation: clip_win_server)(Citation: CISA_AA21_200B) Additionally, adversaries may monitor then replace users' clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining_ruby_reversinglabs) macOS and Linux also have commands, such as `pbpaste`, to grab clipboard contents.(Citation: Operating with EmPyre)

Domain-Name

Value
s1-filecr.xyz
51-83-136-132.xyz

Hostname

Value
websites.theworkpc.com
rec.casacam.net
fon1.sells-it.net
foxn1.sells-it.net
dynsys.is-a-guru.com
srxy123.is-a-geek.com
samaerx.ddnsfree.com

IPv4-Addr

Value
27.1.0.189
108.143.240.80
1.94.147.103
16.1.0.106
14.1.9.124
185.205.209.206
13.70.2.40

External References

- https://otx.alienvault.com/pulse/64be7858d74c880dfcfe7615
- https://decoded.avast.io/martinchlumecky/hotrat-the-risks-of-illegal-software-downloads-and-hidden-autohotkey-script-within/