Sep 07 2023

NETMANAGEIT

Intelligence Report

Cybercriminals target graphic designers with GPU miners

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Cybercriminals are abusing Advanced Installer, a legitimate Windows tool used for creating software packages, to drop cryptocurrency-mining malware on infected machines. This activity has been ongoing since at least November 2021.

Confidence

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

15 / 100

Indicator

Name

51.178.39.184

Description

ISP: OVH SAS **OS:** None ---------- Hostnames: - vps-f70699bf.vps.ovh.net ---------- Domains: - ovh.net ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCqyef9ve8+pUb2qlT9CIBkfVNu1G5BYhOCe/PE3c4ZrBpfmHMjf6p6fUVo8QyJBAL/Scv4v1MyElevqPzvUyD1f/So1+l92Kz53OxqwMcPZt3Z1BFC9KSxVMFTifnqJP9QsRtJFykcJ/RAGi88i4iXn9uIeVkyrx9ZifmC2/sMncWUhCv+rw646/vmBix9X7fgpmhOxszXziUQOhnoqVg3e/wZ0gZEjy6uVoFLoF+yp4EXY0r2UsHYG2ME1P64L489ND3/IXTHtUGgnyxw09iIBXxx14DL5Mc2YLMvSdGiilwVp5gmPp9ZbGs6RkA3g7szsY2hEQdLbB7Ks53Uev5wy+g98x4FTYA/yAxLAU6iw4fihG3TwP15hRVUeThnw8UvTHS4pQy3ha8JFEkTrwpvxCvr+vHJeTnYb1dxFPLIBZi/DKqNWPRhn+pdajByAnjnHdUsSxNBJN1vvbmyGRbKCb3OBfWuweAi6llLknbjumjiriWZCuxJ/MD9FYUXSD8= Fingerprint: 5c:d3:d8:2a:af:ec:11:21:33:8f:a2:6b:9d:ef:9f:ba Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Tue, 05 Sep 2023 06:00:59 GMT Server: Apache/2.4.41 (Ubuntu) Link: ; rel="https://api.w.org/" Link: ; rel="alternate"; type="application/json" Link: ; rel=shortlink Vary: Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '51.178.39.184']

Name

dfa96bee7ba6bf98a9594b568bc8c02012081c8822a5f52d62dd7fac0b0c6974

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dfa96bee7ba6bf98a9594b568bc8c02012081c8822a5f52d62dd7fac0b0c6974']

Name

e559e603702ed249b5c6d057d71be08a1bdba90a19aceaee15d410985c704dde

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e559e603702ed249b5c6d057d71be08a1bdba90a19aceaee15d410985c704dde']

Name

1075c837d0d6b3195c8a2aa2d70419c22ff98e96ebb17ec6e1d1251a5c415db1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1075c837d0d6b3195c8a2aa2d70419c22ff98e96ebb17ec6e1d1251a5c415db1']

Name

3ceb959554450c4ed97bc7c7fbe1d84815a8a3d5be07da9e8d9bb2e705caf9eb

Description

ConventionEngine_Anomaly_MultiPDB_Double

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3ceb959554450c4ed97bc7c7fbe1d84815a8a3d5be07da9e8d9bb2e705caf9eb']

Name

2db2fe6e7b7482f14d5d44446353a277f80afb4905493443a93cc48c1ef120ef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2db2fe6e7b7482f14d5d44446353a277f80afb4905493443a93cc48c1ef120ef']

Name

7a826c7755c173d041f48a08deecc5966082ff274f854174c96cee8c4b7d9d08

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7a826c7755c173d041f48a08deecc5966082ff274f854174c96cee8c4b7d9d08']

Name

29740ff47e77833032744bbbef669755d864da0e1c2a834b903adcb914d6e8a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29740ff47e77833032744bbbef669755d864da0e1c2a834b903adcb914d6e8a6']

Name

99ca71460b7cb4aabde41fed37e647042cfc53bc8dff91aa0a2a28b96c5d2089

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '99ca71460b7cb4aabde41fed37e647042cfc53bc8dff91aa0a2a28b96c5d2089']
Name
b297496f7723c21162e2598f6d914f148c55409197f26a1fe6936f86d566d50d
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b297496f7723c21162e2598f6d914f148c55409197f26a1fe6936f86d566d50d']
Name
c785a3da9a7acca0bc8bcc1de92dfd6647d0bc2f897a1a747b595f89650378e8
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c785a3da9a7acca0bc8bcc1de92dfd6647d0bc2f897a1a747b595f89650378e8']

Name

c0fb29c35a026be5839f10f5a1d889b70107cc836fa894091bf721135f3c6e13

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c0fb29c35a026be5839f10f5a1d889b70107cc836fa894091bf721135f3c6e13']

Name

b133e715a391d653d2c736c95ac8a58cfd37362a77bec4bcce363e61398ffd2b

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b133e715a391d653d2c736c95ac8a58cfd37362a77bec4bcce363e61398ffd2b']

Name

2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73

Description

UPX

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73']

Name

024b6e2e1d8cabb07215686e005e302c5e16e442902225daffe8f1e3382d02d1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '024b6e2e1d8cabb07215686e005e302c5e16e442902225daffe8f1e3382d02d1']

Name

9113b447722ccfcc7b6d6811c3a4f9434c6537697d0bc1cb16966bf8bfbb47c1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9113b447722ccfcc7b6d6811c3a4f9434c6537697d0bc1cb16966bf8bfbb47c1']

Name

3a1fa39b47697402df3eaa56b0e765addeb83f244aeb80ee0bcd434ae98ba5c3

Description

Win64:Malware-gen

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3a1fa39b47697402df3eaa56b0e765addeb83f244aeb80ee0bcd434ae98ba5c3']

Name

b8d323a348aac4e101a3dd0639b2b03d17c2d14f2eba15a70ea0b3e5fb4811a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b8d323a348aac4e101a3dd0639b2b03d17c2d14f2eba15a70ea0b3e5fb4811a9']

Name

e1a272780aa760870a793bde01697ed5f425bbe7f862e85dc06091317f573394

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e1a272780aa760870a793bde01697ed5f425bbe7f862e85dc06091317f573394']

Name

92463ea41e384f462226e473c40f6011d9f9463a05b441782596a2e6d760fe42

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '92463ea41e384f462226e473c40f6011d9f9463a05b441782596a2e6d760fe42']

Name

e6220dcfa3ebaa19c2ef65ca79ac48a9b2a212e142f37e465adac34c112a8a52

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'e6220dcfa3ebaa19c2ef65ca79ac48a9b2a212e142f37e465adac34c112a8a52']
```

Malware

Name
ALF:CERT:Lolminer

Name
PhoenixMiner

Sector

Name
Construction
Description
Private entities engaged in preparation of land and construction, alteration and repair of building, structures and other real estate properties.
Name
Medias and audiovisual
Description
Communication outlets used to deliver information by print, broadcast or Internet and people working in these outlets.
Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.

Attack-Pattern

Name

Process Discovery

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

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

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

Exploitation for Privilege Escalation

ID

T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Resource Hijacking

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to

negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

Name

Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

Command and Scripting Interpreter

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

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts

within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Deobfuscate/Decode Files or Information

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

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

StixFile

Value
b8d323a348aac4e101a3dd0639b2b03d17c2d14f2eba15a70ea0b3e5fb4811a9
e1a272780aa760870a793bde01697ed5f425bbe7f862e85dc06091317f573394
99ca71460b7cb4aabde41fed37e647042cfc53bc8dff91aa0a2a28b96c5d2089
024b6e2e1d8cabb07215686e005e302c5e16e442902225daffe8f1e3382d02d1
9113b447722ccfcc7b6d6811c3a4f9434c6537697d0bc1cb16966bf8bfbb47c1
7a826c7755c173d041f48a08deecc5966082ff274f854174c96cee8c4b7d9d08
2d4adb8e894b22d6c60c3877995ba5e9845ec6005fc95382c395396eb84b1e73
c785a3da9a7acca0bc8bcc1de92dfd6647d0bc2f897a1a747b595f89650378e8
dfa96bee7ba6bf98a9594b568bc8c02012081c8822a5f52d62dd7fac0b0c6974
3ceb959554450c4ed97bc7c7fbe1d84815a8a3d5be07da9e8d9bb2e705caf9eb
b297496f7723c21162e2598f6d914f148c55409197f26a1fe6936f86d566d50d
92463ea41e384f462226e473c40f6011d9f9463a05b441782596a2e6d760fe42
e6220dcfa3ebaa19c2ef65ca79ac48a9b2a212e142f37e465adac34c112a8a52

b133e715a391d653d2c736c95ac8a58cfd37362a77bec4bcce363e61398ffd2b

c0fb29c35a026be5839f10f5a1d889b70107cc836fa894091bf721135f3c6e13

2db2fe6e7b7482f14d5d44446353a277f80afb4905493443a93cc48c1ef120ef

e559e603702ed249b5c6d057d71be08a1bdba90a19aceaee15d410985c704dde

29740ff47e77833032744bbbef669755d864da0e1c2a834b903adcb914d6e8a6

1075c837d0d6b3195c8a2aa2d70419c22ff98e96ebb17ec6e1d1251a5c415db1

3a1fa39b47697402df3eaa56b0e765addeb83f244aeb80ee0bcd434ae98ba5c3

IPv4-Addr

Value
51.178.39.184

External References

- https://otx.alienvault.com/pulse/64fa2102785064eab8350cee
- https://blog.talosintelligence.com/cybercriminals-target-graphic-designers-with-gpu-miners/