Mar 19 2024

NETMANAGEIT

Intelligence Report

Inside the Rabbit Hole: BunnyLoader 3.0 Unveiled

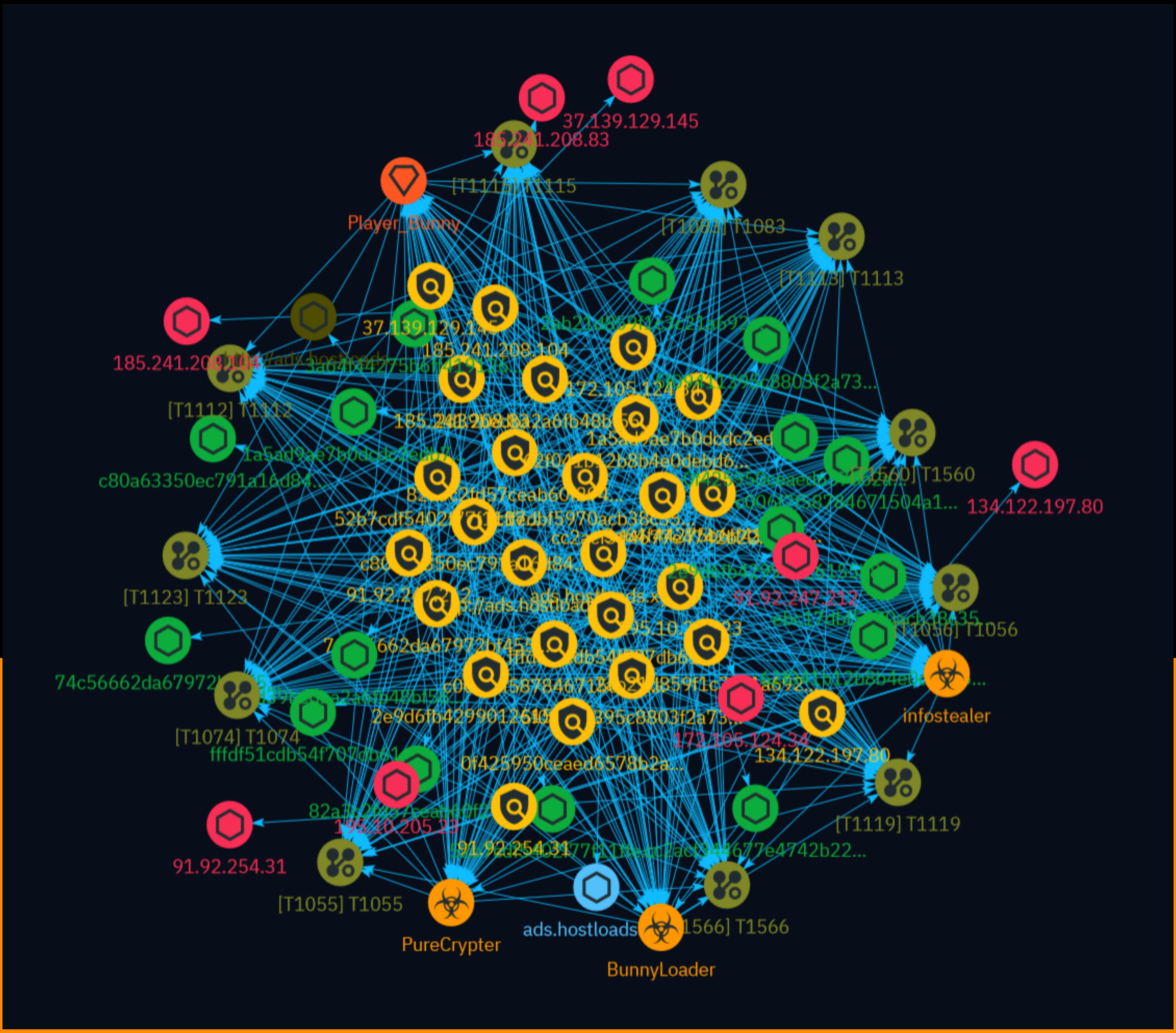

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This article focuses on the newly released BunnyLoader 3.0 malware, its capabilities, and historically observed infrastructure. BunnyLoader is dynamically developing malware that can steal information, credentials, cryptocurrency, and deliver additional malware. The threat actor frequently changes tactics to evade detection and undermine analysis. On Feb. 11, 2024, the threat actor announced BunnyLoader 3.0 with claimed enhancements. Samples show major changes like modularization and updated C2 communication. Revealing evolving tactics empowers defense against this threat.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

ads.hostloads.xyz

Pattern Type

stix

Pattern

[hostname:value = 'ads.hostloads.xyz']

Name

http://ads.hostloads.xyz/BAGUvIxJu32I0/gate.php

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '1 month ago', 'timestamp': 1707747561, 'iso': '2024-02-12T09:19:21-05:00'} - **IPQS: Domain:** ads.hostloads.xyz - **IPQS: IP Address:** 91.92.247.212

Pattern Type

stix

Pattern
[url:value = 'http://ads.hostloads.xyz/BAGUvIxJu32I0/gate.php']
Name
ebc17dbf5970acb38c35e08560ae7b38c7394f503f227575cd56ba1a4c87c8a4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ebc17dbf5970acb38c35e08560ae7b38c7394f503f227575cd56ba1a4c87c8a4']
Name
fffdf51cdb54f707db617b29e2178bb54b67f527c866289887a7ada4d26b7563
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'fffdf51cdb54f707db617b29e2178bb54b67f527c866289887a7ada4d26b7563']
Name
c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a']

Name

cc2acf344677e4742b22725ff310492919499e357a95b609e80eaddc2b155b4b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cc2acf344677e4742b22725ff310492919499e357a95b609e80eaddc2b155b4b']

Name

c006f2f58784671504a1f2e7df8da495759227e64f58657f23efee4f9eb58216

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c006f2f58784671504a1f2e7df8da495759227e64f58657f23efee4f9eb58216']

Name

82a3c2fd57ceab60f2944b6fea352c2aab62b79fb34e3ddc804ae2dbc2464eef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '82a3c2fd57ceab60f2944b6fea352c2aab62b79fb34e3ddc804ae2dbc2464eef']

Name

195.10.205.23

Description

- **Zip Code:** N/A - **ISP:** Reserved - **ASN:** 199417 - **Organization:** Reserved - **Is Crawler:** False - **Timezone:** - **Mobile:** False - **Host:** 195.10.205.23 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** UA - **Region:** N/A - **City:** N/A - **Latitude:** 0 - **Longitude:** 0

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.10.205.23']

Name

74c56662da67972bf4554ff9b23afc5bdab477ba8d4929e1d7dbc608bdc96994

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'74c56662da67972bf4554ff9b23afc5bdab477ba8d4929e1d7dbc608bdc96994']

Name

62f041b12b8b4e0debd6e7e4556b4c6ae7066fa17e67900dcbc991dbd6a8443f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'62f041b12b8b4e0debd6e7e4556b4c6ae7066fa17e67900dcbc991dbd6a8443f']

Name

5f09411395c8803f2a735b71822ad15aa454f47e96fd10acc98da4862524813a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'5f09411395c8803f2a735b71822ad15aa454f47e96fd10acc98da4862524813a']

Name

52b7cdf5402f77f11ffebc2988fc8cdcd727f51a2f87ce3b88a41fd0fb06a124

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '52b7cdf5402f77f11ffebc2988fc8cdcd727f51a2f87ce3b88a41fd0fb06a124']

Name

3a64f44275b6ff41912654ae1a4af1d9c629f94b8062be441902aeff2d38af3e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3a64f44275b6ff41912654ae1a4af1d9c629f94b8062be441902aeff2d38af3e']

Name

2e9d6fb42990126155b8e781f4ba941d54bcc346bcf85b30e3348dde75fbeca1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e9d6fb42990126155b8e781f4ba941d54bcc346bcf85b30e3348dde75fbeca1']

Name

2d39bedba2a6fb48bf56633cc6943edc6fbc86aa15a06c03776f9971a9d2c550

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2d39bedba2a6fb48bf56633cc6943edc6fbc86aa15a06c03776f9971a9d2c550']

Name

2ab21d859f1c3c21a69216c176499c79591da63e1907b0d155f45bb9c6aed4eb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ab21d859f1c3c21a69216c176499c79591da63e1907b0d155f45bb9c6aed4eb']

Name

91.92.247.212

Description

- **Zip Code:** N/A - **ISP:** LIMENET - **ASN:** 394711 - **Organization:** LIMENET - **Is Crawler:** False - **Timezone:** Europe/Sofia - **Mobile:** False - **Host:** 91.92.247.212 - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** BG - **Region:** Sofia (stolitsa) - **City:** Sofia - **Latitude:** 42.7 - **Longitude:** 23.32

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.92.247.212']

Name

1a5ad9ae7b0dcdc2edb7e93556f2c59c84f113879df380d95835fb8ea3914ed8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a5ad9ae7b0dcdc2edb7e93556f2c59c84f113879df380d95835fb8ea3914ed8']

Name

0f425950ceaed6578b2ad22b7baea7d5fe4fd550a97af501bca87d9eb551b825

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f425950ceaed6578b2ad22b7baea7d5fe4fd550a97af501bca87d9eb551b825']

Name

185.241.208.83

Description

- **Zip Code:** N/A - **ISP:** 1337 Services - **ASN:** 210558 - **Organization:** 1337 Services - **Is Crawler:** False - **Timezone:** Europe/Warsaw - **Mobile:** False - **Host:** 185.241.208.83 - **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:** PL - **Region:** Mazovia - **City:** Warsaw - **Latitude:** 52.23 - **Longitude:** 21.01

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.241.208.83']

Name

172.105.124.34

Description

- **Zip Code:** N/A - **ISP:** Akamai Connected Cloud - **ASN:** 63949 - **Organization:** Akamai Connected Cloud - **Is Crawler:** False - **Timezone:** Asia/Singapore - **Mobile:** False - **Host:** 172-105-124-34.ip.linodeusercontent.com - **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:** SG - **Region:** Singapore - **City:** Singapore - **Latitude:** 1.29 - **Longitude:** 103.85

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.105.124.34']

Name

185.241.208.104

Description

- **Zip Code:** N/A - **ISP:** 1337 Services - **ASN:** 210558 - **Organization:** 1337 Services - **Is Crawler:** False - **Timezone:** Europe/Warsaw - **Mobile:** False - **Host:** 185.241.208.104 - **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:** PL - **Region:** Mazovia - **City:** Warsaw - **Latitude:** 52.23 - **Longitude:** 21.01

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.241.208.104']

Name

134.122.197.80

Description

- **Zip Code:** N/A - **ISP:** BGPNET Global - **ASN:** 64050 - **Organization:** BGPNET Global - **Is Crawler:** False - **Timezone:** Asia/Tokyo - **Mobile:** False - **Host:** 134.122.197.80 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** JP - **Region:** Tokyo - **City:** Tokyo - **Latitude:** 35.69 - **Longitude:** 139.69

Pattern Type

stix

Pattern

[ipv4-addr:value = '134.122.197.80']

Name

91.92.254.31

Description

Agressive IP known malicious on AbuseIPDB - countryCode: NL - abuseConfidenceScore: 100 - lastReportedAt: 2023-11-21T14:03:11+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.92.254.31']

Name

37.139.129.145

Description

Quasar RAT botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '37.139.129.145']

Malware

Name
PureCrypter

Name
infostealer

Name
BunnyLoader

Intrusion-Set

Name
Player_Bunny

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
T1074
ID
T1074
Description

Adversaries may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as [Archive Collected Data](https://attack.mitre.org/techniques/T1560). Interactive command shells may be used, and common functionality within [cmd](https://attack.mitre.org/software/S0106) and bash may be used to copy data into a staging location.(Citation: PWC Cloud Hopper April 2017) In cloud environments, adversaries may stage data within a particular instance or virtual machine before exfiltration. An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002) and stage data in that instance.(Citation: Mandiant M-Trends 2020) Adversaries may choose to stage data from a victim network in a centralized location prior to Exfiltration to minimize the number of connections made to their C2 server and better evade detection.

Name

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name

T1566

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

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

T1560

ID

T1560

Description

An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender. Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

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

T1115

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)

Name

T1119

ID

T1119

Description

Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. In cloud-based environments, adversaries may also use cloud APIs, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data. This functionality could also be built into remote access tools. This technique may incorporate use of other techniques such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) and [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570) to identify and move files, as well as [Cloud Service Dashboard](https://attack.mitre.org/techniques/T1538) and [Cloud Storage Object Discovery](https://attack.mitre.org/techniques/T1619) to identify resources in cloud environments.

Name

T1123

ID

T1123

Description

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information. Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

Name

T1113

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)

Hostname

Value
ads.hostloads.xyz

Url

Value
http://ads.hostloads.xyz/BAGUvIxJu32I0/gate.php

IPv4-Addr

Value
91.92.247.212
195.10.205.23
185.241.208.83
172.105.124.34
185.241.208.104
134.122.197.80
91.92.254.31
37.139.129.145

StixFile

Value
ebc17dbf5970acb38c35e08560ae7b38c7394f503f227575cd56ba1a4c87c8a4
fffdf51cdb54f707db617b29e2178bb54b67f527c866289887a7ada4d26b7563
cc2acf344677e4742b22725ff310492919499e357a95b609e80eaddc2b155b4b
c80a63350ec791a16d84b759da72e043891b739a04c7c1709af83da00f7fdc3a
c006f2f58784671504a1f2e7df8da495759227e64f58657f23efee4f9eb58216
82a3c2fd57ceab60f2944b6fea352c2aab62b79fb34e3ddc804ae2dbc2464eef
62f041b12b8b4e0debd6e7e4556b4c6ae7066fa17e67900dcbc991dbd6a8443f
74c56662da67972bf4554ff9b23afc5bdab477ba8d4929e1d7dbc608bdc96994
5f09411395c8803f2a735b71822ad15aa454f47e96fd10acc98da4862524813a
52b7cdf5402f77f11ffebc2988fc8cdcd727f51a2f87ce3b88a41fd0fb06a124
3a64f44275b6ff41912654ae1a4af1d9c629f94b8062be441902aeff2d38af3e
2e9d6fb42990126155b8e781f4ba941d54bcc346bcf85b30e3348dde75fbeca1
2d39bedba2a6fb48bf56633cc6943edc6fbc86aa15a06c03776f9971a9d2c550

2ab21d859f1c3c21a69216c176499c79591da63e1907b0d155f45bb9c6aed4eb
1a5ad9ae7b0dcdc2edb7e93556f2c59c84f113879df380d95835fb8ea3914ed8
0f425950ceaed6578b2ad22b7baea7d5fe4fd550a97af501bca87d9eb551b825

External References

- https://unit42.paloaltonetworks.com/analysis-of-bunnyloader-malware/#post-132991-_v8176g40kstn
- https://otx.alienvault.com/pulse/65f8166603c2a38b78d1698e