Jun 27 2024

NETMANAGEIT

Intelligence Report

New InnoSetup Malware Created Upon Each Download Attempt

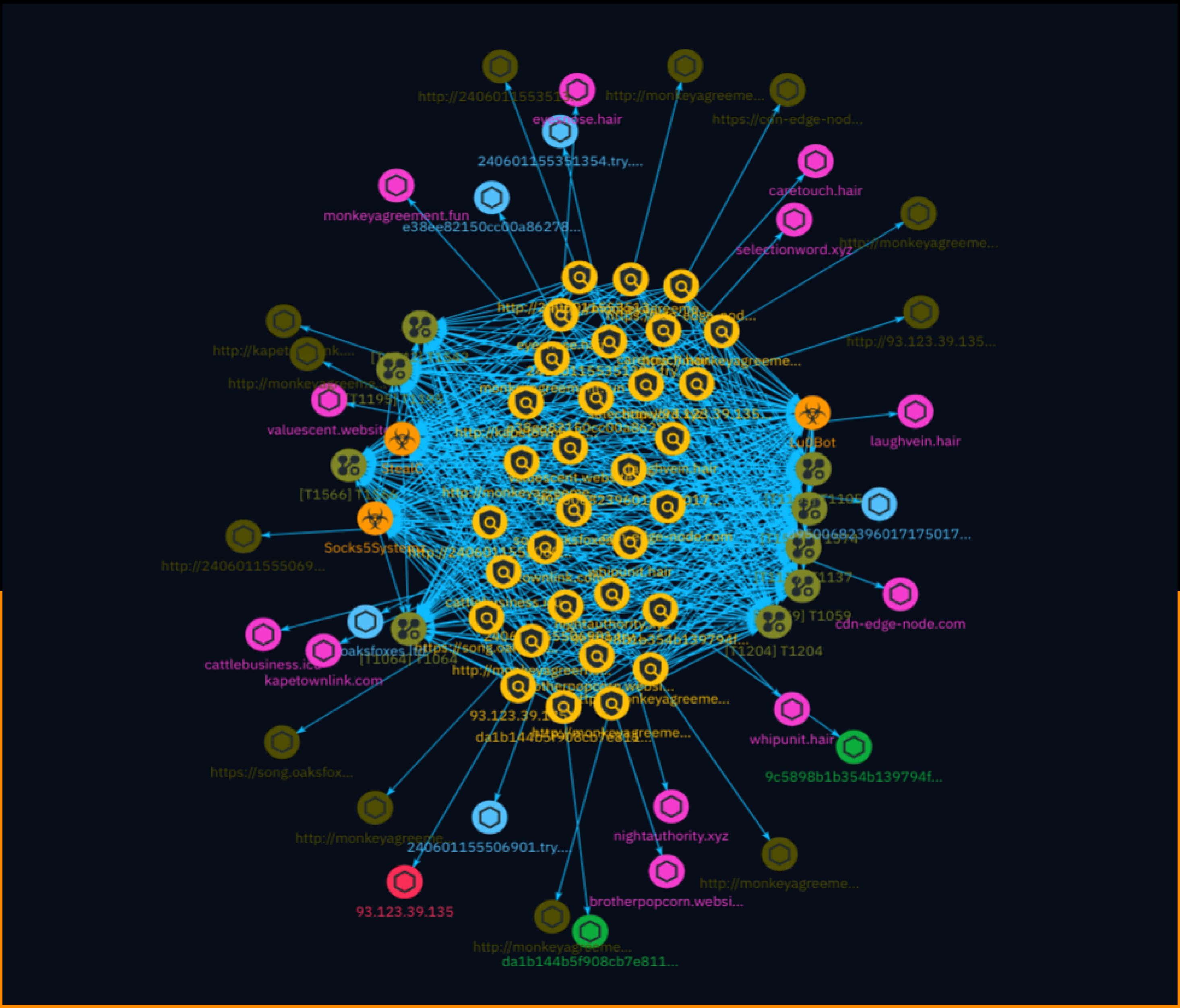

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A security intelligence report describing a new malware distribution technique where malicious code is dynamically generated for each download attempt, evading detection through unique hash values. The malware, termed 'InnoLoader', disguises itself as legitimate software installers, executing a complex sequence of downloading and executing additional payloads, including information stealers, adware, and malicious browser plugins. It employs evasion tactics like varying C2 responses and downloading benign files to hinder analysis. The report underscores the evolving strategies employed by threat actors to distribute malware and compromise systems.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name

T1064

ID

T1064

Description

This technique has been deprecated. Please use [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) where appropriate. Adversaries may use scripts to aid in operations and perform multiple actions that would otherwise be manual. Scripting is useful for speeding up operational tasks and reducing the time required to gain access to critical resources. Some scripting languages may be used to bypass process monitoring mechanisms by directly interacting with the operating system at an API level instead of calling other programs. Common scripting languages for Windows include VBScript and [PowerShell](https://attack.mitre.org/techniques/T1086) but could also be in the form of command-line batch scripts. Scripts can be embedded inside Office documents as macros that can be set to execute when files used in [Spearphishing Attachment](https://attack.mitre.org/techniques/T1193) and other types of spearphishing are opened. Malicious embedded macros are an alternative means of execution than software exploitation through [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203), where adversaries will rely on macros being allowed or that the user will accept to activate them. Many popular offensive frameworks exist which use forms of scripting for security testers and adversaries alike. Metasploit (Citation: Metasploit_Ref), Veil (Citation: Veil_Ref), and PowerSploit (Citation: Powersploit) are three examples that are popular among penetration testers for exploit and post-compromise operations and include many features for evading defenses. Some adversaries are known to use PowerShell. (Citation: Alperovitch 2014)

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

T1137

ID

T1137

Description

Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins. A variety of features have been discovered in Outlook that can be abused to obtain persistence, such as Outlook rules, forms, and Home Page.(Citation: SensePost Ruler GitHub) These persistence mechanisms can work within Outlook or be used through Office 365.(Citation: TechNet O365 Outlook Rules)

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; running malicious JavaScript in their browser, allowing adversaries to [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)s; or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204).(Citation: Talos Roblox Scam 2023)(Citation: Krebs Discord Bookmarks 2023) 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

T1574

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

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`.(Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://attack.mitre.org/techniques/T1204) (typically after interacting with [Phishing](https://attack.mitre.org/techniques/T1566) lures).(Citation: T1105: Trellix_search-ms) Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1542

ID

T1542

Description

Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system. During the booting process of a computer, firmware and various startup services are loaded before the operating system. These programs control flow of execution before the operating system takes control.(Citation: Wikipedia Booting) Adversaries may overwrite data in boot drivers or firmware such as BIOS (Basic Input/Output System) and The Unified Extensible Firmware Interface (UEFI) to persist on systems at a layer below the operating system. This can be particularly difficult to detect as malware at this level will not be detected by host software-based defenses.

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

T1195

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Indicator

Name

93.123.39.135

Pattern Type

stix

Pattern

[ipv4-addr:value = '93.123.39.135']

Name

monkeyagreement.fun

Pattern Type

stix

Pattern

[domain-name:value = 'monkeyagreement.fun']

Name

240601155506901.try.kyhd08.buzz

Pattern Type

stix

Pattern

[hostname:value = '240601155506901.try.kyhd08.buzz']

Name

https://song.oaksfoxes.ltd/tid/202.exe

Pattern Type

stix

Pattern

[url:value = 'https://song.oaksfoxes.ltd/tid/202.exe']

Name

240601155351354.try.kyhd08.buzz

Pattern Type

stix

Pattern

[hostname:value = '240601155351354.try.kyhd08.buzz']

Name

song.oaksfoxes.ltd

Pattern Type

stix

Pattern

[hostname:value = 'song.oaksfoxes.ltd']

Name

https://cdn-edge-node.com/online_security_mkl.exe

Pattern Type

stix

Pattern

[url:value = 'https://cdn-edge-node.com/online_security_mkl.exe']

Name

caretouch.hair

Pattern Type

stix

Pattern

[domain-name:value = 'caretouch.hair']

Name

http://monkeyagreement.fun/coo.php?paw=762694&spot=2&a=2857&on=458&o=1688

Pattern Type
stix
Pattern
[url:value = 'http://monkeyagreement.fun/coo.php?paw=762694&spot=2&a=2857&on=458&o=1688']
Name
d9500682396017175017969210108a04a635094d7af3f018356690047bce5.aoa.aent78.sbs
Pattern Type
stix
Pattern
[hostname:value = 'd9500682396017175017969210108a04a635094d7af3f018356690047bce5.aoa.aent78.sbs']
Name
cdn-edge-node.com
Pattern Type
stix
Pattern
[domain-name:value = 'cdn-edge-node.com']
Name

da1b144b5f908cb7e811489dfe660e06aa6df9c9158c6972ec9c79c48afacb7e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da1b144b5f908cb7e811489dfe660e06aa6df9c9158c6972ec9c79c48afacb7e']

Name

http://93.123.39.135/129edec4272dc2c8.php

Pattern Type

stix

Pattern

[url:value = 'http://93.123.39.135/129edec4272dc2c8.php']

Name

brotherpopcorn.website

Pattern Type

stix

Pattern

[domain-name:value = 'brotherpopcorn.website']

Name
http://monkeyagreement.fun/coo.php?paw=883174&spot=1&a=2857&on=444&o=1678
Pattern Type
stix
Pattern
[url:value = 'http://monkeyagreement.fun/coo.php?paw=883174&spot=1&a=2857&on=444&o=1678']

Name
selectionword.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'selectionword.xyz']

Name
http://monkeyagreement.fun/coo.php?paw=787557&spot=6&a=2857&on=244&o=331
Pattern Type
stix
Pattern

[url:value = 'http://monkeyagreement.fun/coo.php?paw=787557&spot=6&a=2857&on=244&o=331']

Name

nightauthority.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'nightauthority.xyz']

Name

laughvein.hair

Pattern Type

stix

Pattern

[domain-name:value = 'laughvein.hair']

Name

kapetownlink.com

Pattern Type

stix

Pattern

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

Name

e38ee82150cc00a8627814c6.bag.sack54.net

Pattern Type

stix

Pattern

[hostname:value = 'e38ee82150cc00a8627814c6.bag.sack54.net']

Name

9c5898b1b354b139794f10594e84e94e991971a54d179b2e9f746319ffac56aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9c5898b1b354b139794f10594e84e94e991971a54d179b2e9f746319ffac56aa']

Name

eyesnose.hair

Pattern Type

stix

Pattern

[domain-name:value = 'eyesnose.hair']

Name

valuescent.website

Pattern Type

stix

Pattern

[domain-name:value = 'valuescent.website']

Name

http://monkeyagreement.fun/coo.php?paw=401610&spot=3&a=2857&on=420&o=1662

Pattern Type

stix

Pattern

[url:value = 'http://monkeyagreement.fun/coo.php?paw=401610&spot=3&a=2857&on=420&o=1662']

Name

http://kapetownlink.com/installer.exe

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '2 years ago', 'timestamp': 1652207986, 'iso': '2022-05-10T14:39:46-04:00'} - **IPQS: Domain:** kapetownlink.com - **IPQS: IP Address:** 159.223.29.40

Pattern Type

stix

Pattern

[url:value = 'http://kapetownlink.com/installer.exe']

Name

http://monkeyagreement.fun/coo.php?paw=956684&spot=5&a=2857&on=460&o=1690

Pattern Type

stix

Pattern

[url:value = 'http://monkeyagreement.fun/coo.php?paw=956684&spot=5&a=2857&on=460&o=1690']

Name

http://240601155351354.try.kyhd08.buzz/f/fvgbm0601001.msi

Pattern Type

stix

Pattern

[url:value = 'http://240601155351354.try.kyhd08.buzz/f/fvgbm0601001.msi']

Name

http://240601155506901.try.kyhd08.buzz/f/fvgbm0601901.txt

Pattern Type

stix

Pattern

[url:value = 'http://240601155506901.try.kyhd08.buzz/f/fvgbm0601901.txt']

Name

cattlebusiness.icu

Pattern Type

stix

Pattern

[domain-name:value = 'cattlebusiness.icu']

Name

whipunit.hair

Pattern Type

stix

Pattern

[domain-name:value = 'whipunit.hair']

Name

http://monkeyagreement.fun/coo.php?paw=895836&spot=4&a=2857&on=418&o=1660

Pattern Type

stix

Pattern

[url:value = 'http://monkeyagreement.fun/coo.php?paw=895836&spot=4&a=2857&on=418&o=1660']

Malware

Name
Socks5Systemz

Name
StealC

Name
Lu0Bot

indicates

Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

indicates

uses

Name

based-on

Name

Name

Name

Name

Domain-Name

Value
nightauthority.xyz
brotherpopcorn.website
cdn-edge-node.com
monkeyagreement.fun
kapetownlink.com
valuescent.website
eyesnose.hair
cattlebusiness.icu
selectionword.xyz
whipunit.hair
laughvein.hair
caretouch.hair

StixFile

Value
da1b144b5f908cb7e811489dfe660e06aa6df9c9158c6972ec9c79c48afacb7e
9c5898b1b354b139794f10594e84e94e991971a54d179b2e9f746319ffac56aa

Hostname

Value
song.oaksfoxes.ltd
240601155506901.try.kyhd08.buzz
e38ee82150cc00a8627814c6.bag.sack54.net
d9500682396017175017969210108a04a635094d7af3f018356690047bce5.aoa.aent78.sbs
240601155351354.try.kyhd08.buzz

IPv4-Addr

Value
93.123.39.135

External References

- https://asec.ahnlab.com/en/67502/
- https://otx.alienvault.com/pulse/667d322126c4b8db836d56aa