Aug 08 2023

NETMANAGEIT

Intelligence Report

Latest Batloader Campaigns Use Pyarmor Pro for Evasion

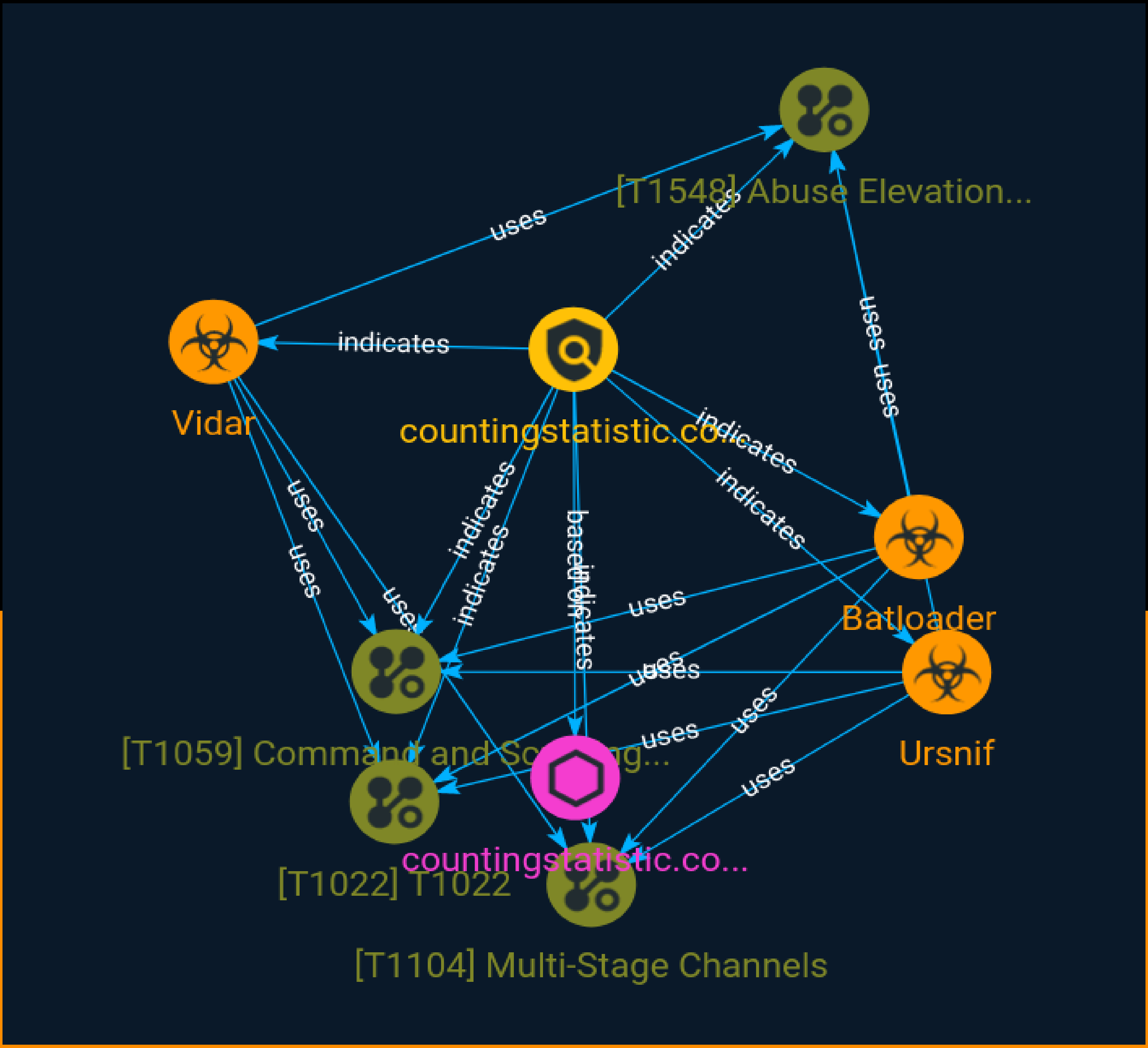

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In June 2023, Trend Micro observed an upgrade to the evasion techniques used by the Batloader initial access malware, the group behind Batloader (which we named Water Minyades) have begun employing Pyarmor Pro — a more sophisticated version of the regular Pyarmor protector command-line tool — to obfuscate its main malicious python scripts.

Confidence

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

15 / 100

Indicator

Name	countingstatistic.com
Pattern Type	stix
Pattern	[domain-name:value = 'countingstatistic.com']

Malware

Name
Batloader

Name
Vidar

Name
Ursnif

Description
[Ursnif](https://attack.mitre.org/software/S0386) is a banking trojan and variant of the Gozi malware observed being spread through various automated exploit kits, [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001)s, and malicious links.(Citation: NJCCIC Ursnif Sept 2016)(Citation: ProofPoint Ursnif Aug 2016) [Ursnif](https://attack.mitre.org/software/S0386) is associated primarily with data theft, but variants also include components (backdoors, spyware, file injectors, etc.) capable of a wide variety of behaviors.(Citation: TrendMicro Ursnif Mar 2015)

Attack-Pattern

Name

T1022

ID

T1022

Name

Abuse Elevation Control Mechanism

ID

T1548

Description

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

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

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)

Domain-Name

Value
countingstatistic.com

External References

- https://otx.alienvault.com/pulse/64d13db4c73971185ff3c8ec
- https://www.trendmicro.com/en_us/research/23/h/batloader-campaigns-use-pyarmor-pro-for-evasion.html
- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/h/latest-batloader-campaigns-use-pyarmor-pro-for-evasion/ioc-latest-batloader-campaigns-use-pyarmor-pro-for-evasion.txt