



NETMANAGEIT

Intelligence Report

CloudWizard APT: the bad magic story goes on

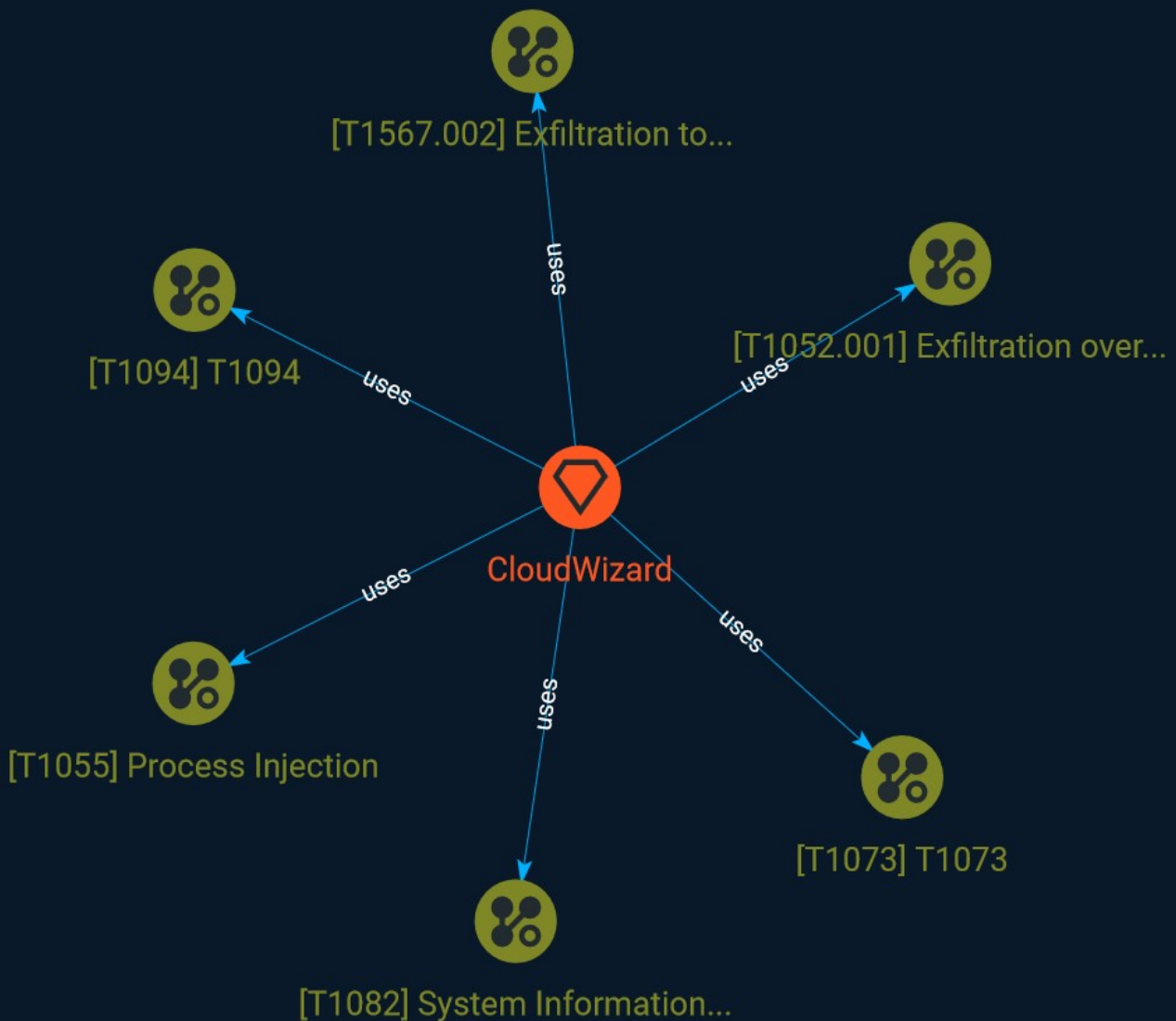


Table of contents

Overview

● Description	3
● Confidence	3

Entities

● Attack-Pattern	4
● Intrusion-Set	7

External References

● External References	8
-----------------------	---

Overview

Description

In March 2023, we uncovered a previously unknown APT campaign in the region of the Russo-Ukrainian conflict that involved the use of PowerMagic and CommonMagic implants. However, at the time it was not clear which threat actor was behind the attack. Since the release of our report about CommonMagic, we have been looking for additional clues that would allow us to learn more about this actor. As we expected, we have been able to gain a deeper insight into the “bad magic” story.

Confidence

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

15 / 100

Attack-Pattern

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

Exfiltration to Cloud Storage

ID

T1567.002

Description

Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet. Examples of cloud storage services include Dropbox and Google Docs. Exfiltration to these cloud storage services can provide a significant amount of cover to the adversary if hosts within the network are already communicating with the service.

Name

T1073

ID

T1073

Name

T1094

ID

T1094

Name

Exfiltration over USB

ID

T1052.001

Description

Adversaries may attempt to exfiltrate data over a USB connected physical device. In certain circumstances, such as an air-gapped network compromise, exfiltration could occur via a USB device introduced by a user. The USB device could be used as the final exfiltration point or to hop between otherwise disconnected systems.

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virtual Machine API)

Intrusion-Set

Name
CloudWizard

External References

-
- <https://otx.alienvault.com/pulse/6467a7ac79c273e1aeab8999>