2024-06-18

HUNTER

EMERGING THREATS

HUNTING FOR CREDENTIAL THEFT – IDENTIFY WHEN AN INFOSTEALER MAY BE STEALING SENSITIVE ACCESS

The recent SnowFlake incident has brought to light the importance of protecting your credentials and access to sensitive tools. Infostealers are the highway in which many threat actors and access brokers garner their initial foothold in environments. This collection of hunt packages has been specifically put together to help organizations and teams detect and prevent info stealing malware from operating within their environment. This variant of malware is normally designed to steal sensitive information from victimized systems. The info or data stolen typically include proprietary/personal information, login credentials, financial data, and other data that a victim would consider confidential. The first infostealer malware was discovered in 2006 and was known as ZeuS (or Zbot). It was used to steal banking credentials, eventually leading to banking fraud and malicious botnets. Since then, infostealer malware has evolved and many different variants with the same agenda have appeared in the wild. Most recently, utilizing [Intel 471](https://intel471.com/)'s reliable threat intelligence, it was reported of the compromising of hundreds of Snowflake instances that were accessed via credentials taken with Infostealer malware - individuals reportedly targeted didn't have MFA enabled, thus were susceptible to compromise. The major consequences of infection can result in the loss of sensitive data, persistent espionage and/or financial losses to the targeted victims. This type of malware has been around for a sustained period of time and has no reason to fade away, due to its functionality and usefulness to threat actors. Therefore, the understanding of and preparation for such infections should be taken seriously in any environment.

THREAT SUMMARY

The recent SnowFlake incident has brought to light the importance of protecting your credentials and access to sensitive tools. Infostealers are the highway in which many threat actors and access brokers garner their initial foothold in environments. This collection of hunt packages has been specifically put together to help organizations and teams detect and prevent info stealing malware from operating within their environment. This variant of malware is normally designed to steal sensitive information from victimized systems. The info or data stolen typically include proprietary/personal information, login credentials, financial data, and other data that a victim would consider confidential. The first infostealer malware was discovered in 2006 and was known as ZeuS (or Zbot). It was used to steal banking credentials, eventually leading to banking fraud and malicious botnets. Since then, infostealer malware has evolved and many different variants with the same agenda have appeared in the wild. Most recently, utilizing [Intel 471](https://intel471.com/)'s reliable threat intelligence, it was reported of the compromising of hundreds of Snowflake instances that were accessed via credentials taken with Infostealer malware - individuals reportedly targeted didn't have MFA enabled, thus were susceptible to compromise. The major consequences of infection can result in the loss of sensitive data, persistent espionage and/or financial losses to the targeted victims. This type of malware has been around for a sustained period of time and has no reason to fade away, due to its functionality and usefulness to threat actors. Therefore, the understanding of and preparation for such infections should be taken seriously in any environment.

Intel 471 References:

[TITAN Intelligence Report: Several high-profile compromises impact Snowflake cloud storage provider customers](https://titan.intel471.com/report/fintel/b818896a10231db287121eb786a022f5)

[TITAN Information Report: Actorsâ€™ claims possibly related to Snowflake account takeover campaign](https://titan.intel471.com/report/inforep/0df4d459d7d042c5ece3c3cb5b0062f2)

SYNOPSIS

This collection of information-stealing malware hunt packages gives analysts visibility into the tactics, techniques and procedures (TTPs) that may be observed when infected with this classification of malware. Information-stealer malware was distributed via a variety of methods, which include phishing emails, malicious attachments or documents, infected websites and even vulnerabilities within software that can be exploited. With a system already compromised, information stealers use a number of techniques to retrieve the sensitive information that they seek from their victims. These techniques include key logging, form grabbing, clipboard hijacking, email harvesting, web-injection scripts, screen captures and credential theft. Due to most infections coinciding with command and control (C2) communication and/or updates, operators typically utilize obfuscated and encrypted transmission of stolen data with these servers. With the exfiltrated data more than likely being utilized for further stages of infection or sold in the cyber underground, the proliferation of stealthy and effective information-stealer malware can cause havoc across organizations. Strains such as Zeus, Ursnif, LokiBot, Raccoon Stealer, Vidar, and Redline Stealer â€" the last two were observed in the recent Snowflake attacks â€" and are just a few examples of the large number of information-stealer malware variations that an analyst may encounter and should be aware of as they hunt in their environment.

HUNT PACKAGES

POTENTIALLY INJECTED PROCESS COMMAND EXECUTION
https://hunter.cyborgsecurity.io/research/hunt-package/7daf20ca-9558-4b09-bb38-03a09e47746b

DEFENDER BYPASS VIA REGISTRY KEY CHANGES
https://hunter.cyborgsecurity.io/research/hunt-package/c4c811f9-9180-409d-aae8-95b42bb52e5f

AUTORUN OR ASEP REGISTRY KEY MODIFICATION
https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

SUSPICIOUS FILE CREATION IN ONENOTE EXPORTED FILE FOLDERS – POTENTIAL ONENOTE PHISHING
https://hunter.cyborgsecurity.io/research/hunt-package/2F7B9F4B-E6C8-42BB-8539-AF10C8316590

EXECUTING SYSTEM32 DIRECTORY EXECUTABLES FOR MASQUERADING
https://hunter.cyborgsecurity.io/research/hunt-package/f6bc5220-3b4e-4137-916f-e11487ab3f23

EXCESSIVE WINDOWS DISCOVERY AND EXECUTION PROCESSES – POTENTIAL MALWARE INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/6d1c9f13-e43e-4b52-a443-5799465d573b

MASQUERADING PROCESS OUTSIDE OF NATIVE DIRECTORY
https://hunter.cyborgsecurity.io/research/hunt-package/cd35dde0-2e10-4b8d-977f-5571abb3a4fb

SCHEDULED TASK CREATED
https://hunter.cyborgsecurity.io/research/hunt-package/aaa77f56-4a4c-4fdd-a6e3-156e1996d310

MICROSOFT MALWARE PROTECTION ENGINE (MSMPENG) EXECUTED FROM NON-STANDARD DIRECTORY – POTENTIAL MASQUERADING OR DLL SIDE-LOADING
https://hunter.cyborgsecurity.io/research/hunt-package/4becf4df-456b-4503-8a50-d9ed6028f55e

SUSPICIOUS ONENOTE EXPORTED FILE IN COMMAND EXECUTION – POTENTIAL ONENOTE PHISHING
https://hunter.cyborgsecurity.io/research/hunt-package/49707171-F77A-4CD3-8096-F38CDBDE98B2

COMMON ABUSED EXECUTABLES LAUNCHED OUTSIDE OF SYSTEM32
https://hunter.cyborgsecurity.io/research/hunt-package/50641742-9446-4418-a0fa-9ac0fdb9d7dc

RELATED LINKS
Sign up for free HUNTER access
Hunting for Credential Theft - Identify When an InfoStealer May be Stealing Sensitive Access Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Privilege Escalation
  - Persistence
  - Initial Access
  - Discovery
  - Defense Evasion
  - Execution
- Technique Names:
  - Mshta
  - Registry Run Keys / Startup Folder
  - Scheduled Task/Job
  - Match Legitimate Name or Location
  - Process Injection
  - PowerShell
  - Windows Command Shell
  - DLL Side-Loading
  - Masquerading
  - Phishing
  - JavaScript
  - Malicious File
  - Visual Basic
  - Disable or Modify Tools
  - System Network Configuration Discovery
- Threat Names:
  - Vidar
  - Ursnif
  - RedLine Stealer

REFERENCES

1. https://www.malwarebytes.com/blog/threats/info-stealers
2. https://www.accenture.com/us-en/blogs/security/information-stealer-malware-on-dark-web
3. https://www.packetlabs.net/posts/what-is-infostealer-malware-and-how-does-it-work/
4. https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
5. https://titan.intel471.com/report/fintel/b818896a10231db287121eb786a022f5
6. https://titan.intel471.com/report/inforep/0df4d459d7d042c5ece3c3cb5b0062f2