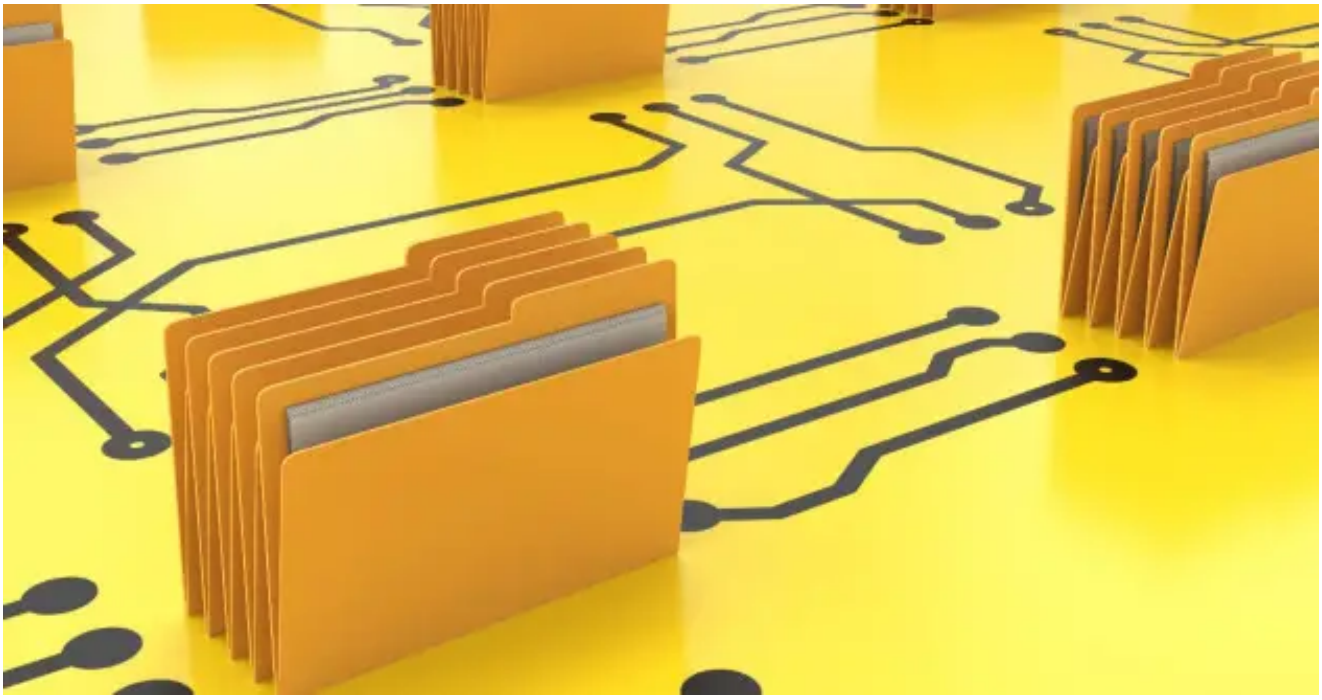
X-Force Prevents Zero Day from Going Anywhere

securityintelligence.com/posts/x-force-prevents-zero-day-from-going-anywhere



Software Vulnerabilities March 30, 2023
By John Dwyer 8 min read
This blog was made possible through contributions from Fred Chidsey and Joseph Lozowski.

The 2023 X-Force Threat Intelligence Index shows that vulnerability discovery has rapidly increased year-over-year and according to X-Force's cumulative vulnerability and exploit database, only 3% of vulnerabilities are associated with a zero day. X-Force often observes zero-day exploitation on Internet-facing systems as a vector for initial access however, X-Force has also observed zero-day attacks leveraged by attackers to accomplish their goals and objectives after initial access was obtained.

In this post, X-Force will detail an investigation associated with a zero-day attack that occurred less than 24 hours after the release of the zero day — one of the fastest adoption times for financially motivated cybercriminals identified by X-Force since 2020. This incident is connected to a recent mass ransomware attack, which takes advantage of a vulnerability in Forta's file-transfer tool, GoAnyWhere.

This blog will also explore the relationship between ransomware attack paths and the adoption of zero days by cybercriminals: by analyzing the most commonly used zero-day exploits by cybercriminals observed by X-Force over the last three years, we've found that the ransomware attack lifecycle is a key driver behind zero-day adoption for cyber criminals.

GoAnyWhere But Laterally

In February 2023, X-Force responded to an incident where a client had received alerts from their security tooling regarding potential lateral movement originating from a server within their network. The client's security team discovered an authorized user account operating on a GoAnyWhere MFT server. Through analysis of existing security telemetry and forensic evidence, X-Force identified evidence of post-exploitation activity and exploitation of CVE-2023-0669 on the GoAnyWhere MFT server.

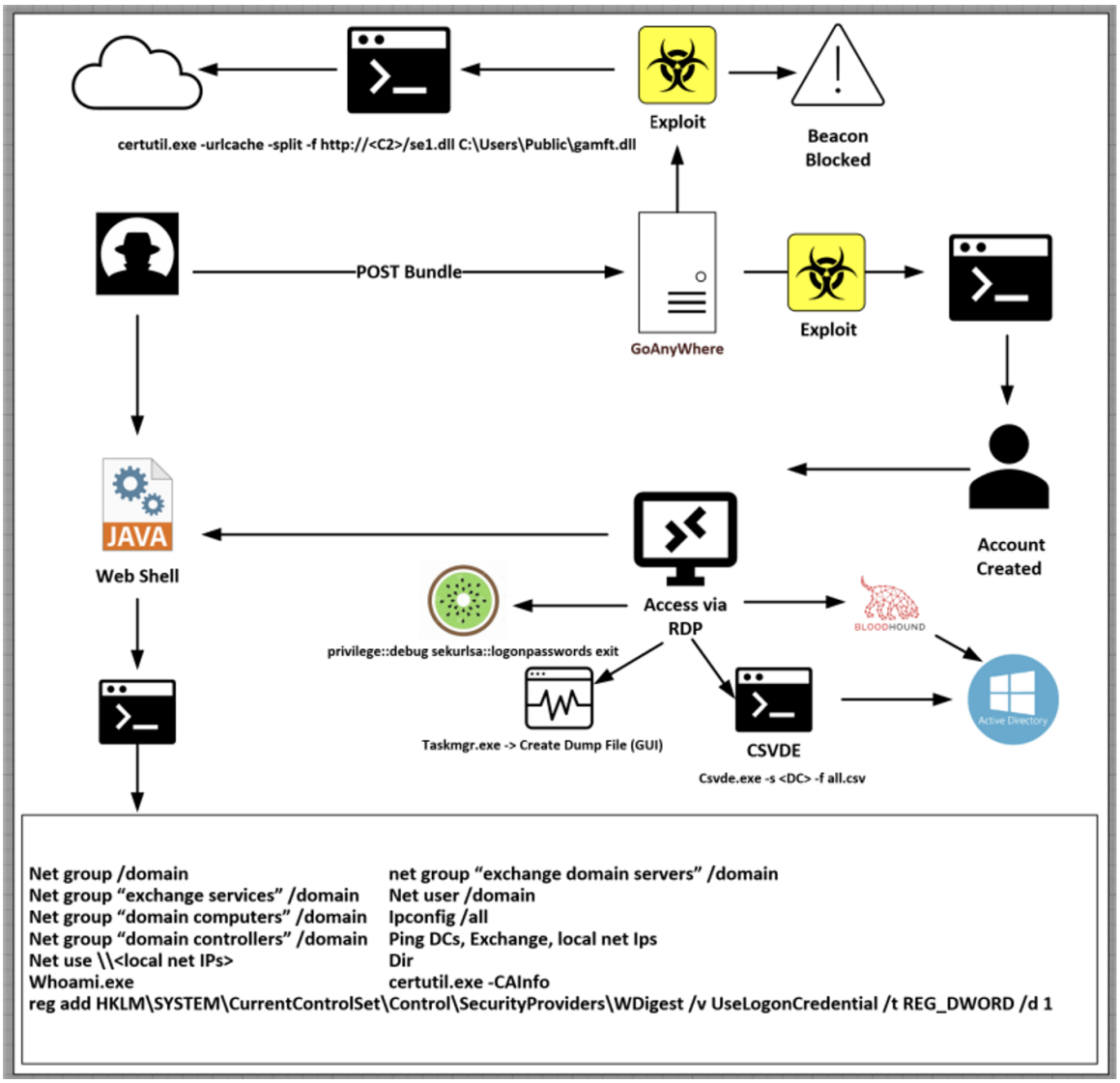
X-Force uncovered exploitation of CVE-2023-0669 through timeline analysis indicating a common post-exploitation command to download a file from a remote IP address was executed on the GoAnyWhere server at the same time a GoAnyWhere license error log was written referencing the same remote IP address. Upon first exploitation, the attacker attempted to download and execute a malicious payload which would have established a command and control (C2) channel via a Cobalt Strike but the security tooling on the GoAnyWhere server detected and removed the malicious payload. X-Force recovered similar evidence indicating that the attacker attempted to execute Mimikatz through the exploitation of the vulnerability and was prevented.

With security tooling blocking the execution of remote post-exploitation commands, the attacker pivoted to interactive access via remote desktop protocol (RDP) by leveraging the vulnerability to create a new user account and then accessing the server via RDP. With interactive access to the server via RDP, the attacker continued with credential harvesting operations by accessing credential data using Task Manager to dump the contents of the LSASS process.

Following the credential harvesting operations, the attacker began internal reconnaissance focusing on Active Directory using CSVDE and scanning for accessible SMB shares. Comma Separated Value Directory Exchange (CSVDE) is Microsoft Windows utility that enables the user to import and export objects into or from Active Directory.

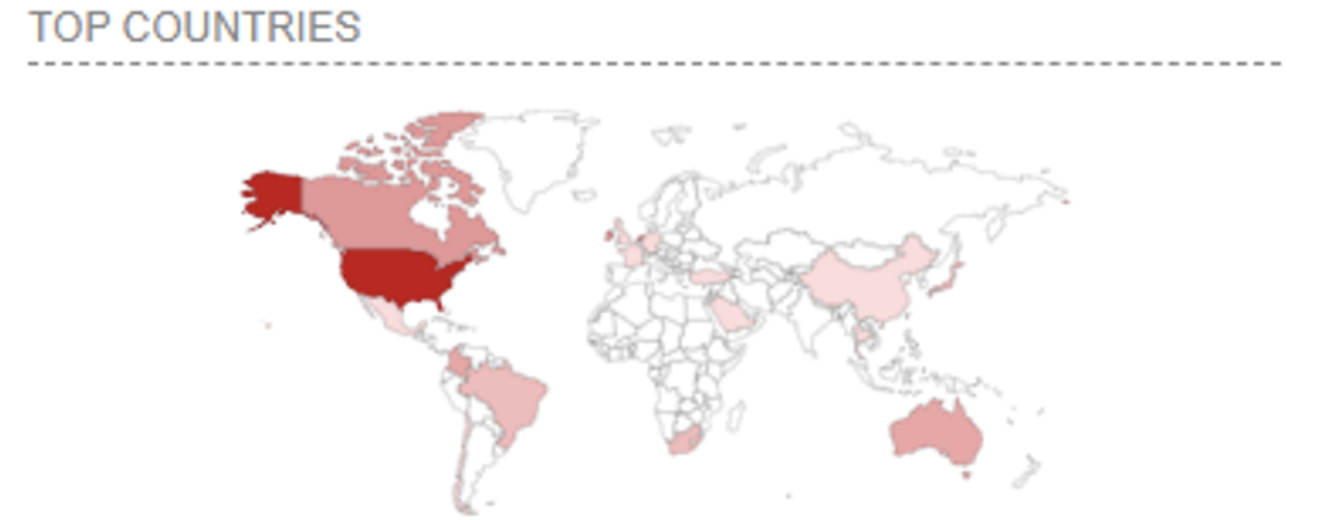
The attacker pivoted C2 channels by uploading a web shell to the GoAnyWhere server and began executing point-exploitation commands focused on reconnaissance and user account creation. When the web shell was detected and contained, the attacker returned to the server through RDP and performed more credential harvesting activities and leveraged SharpHound to perform additional Active Directory data collections. SharpHound is a component of BloodHound which is an Active Directory reconnaissance tool designed to enumerate and analyze Active Directory relationships and attack paths.

With an understanding of the attacker's access and scope of the incident in place, containment actions were taken to remove the attack from the network completely. Further intelligence gathering of the data collected from the incident indicates that the attacker was a financially motivated attacker focused on ransomware attacks to extort payment.

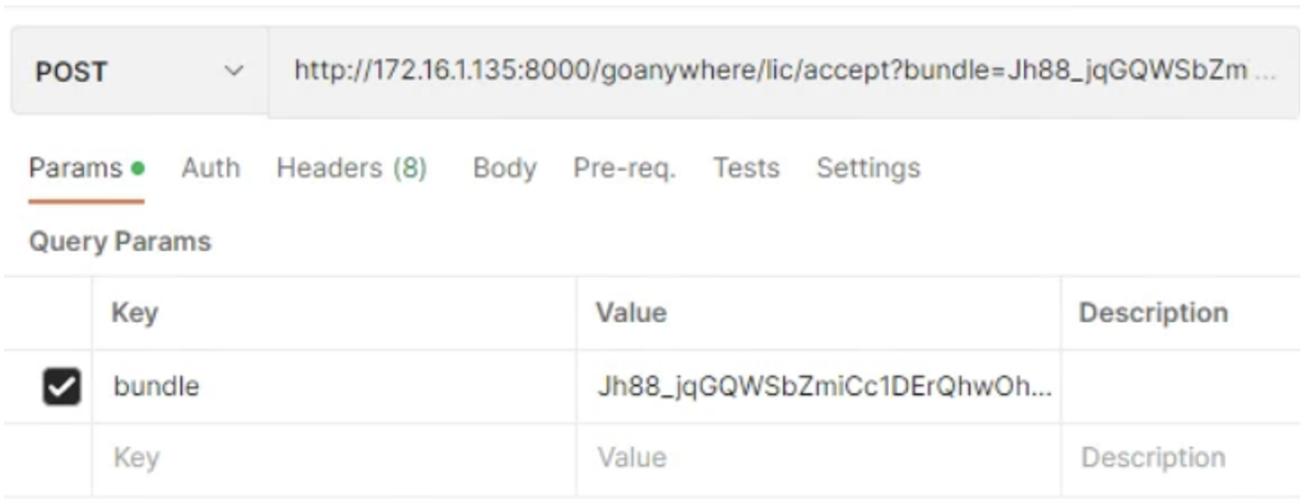


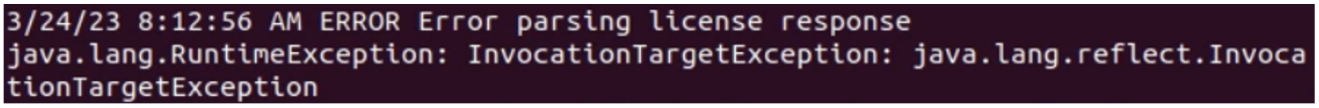
Detecting CVE-2023-0669

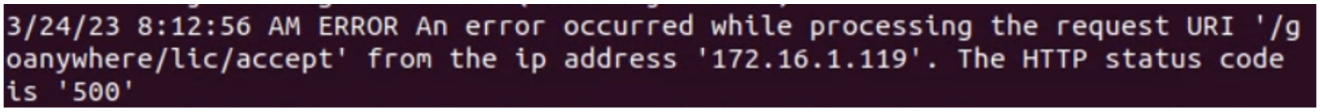
CVE-2023-0669 is a remote code injection vulnerability impacting Fortra's GoAnyWhere MFT file transfer software. The vulnerability enables a remote attacker with access to the administrative console to inject pre-authentication commands in the License Response Servlet. Exploitation of CVE-2023-0669 occurs when a remote attacker sends a specially crafted request to the URI "/goanywhere/lic/accept" to take advantage of an insecure deserialization flaw in the License Response Servlet class. Due to the use of hard-coded keys within the source code of the GoAnyWhere functions, a remote attacker can encrypt and encode arbitrary commands for execution on the target system within the Bundle parameter which is processed by the License Server Servlet without authentication. It is important to note that this exploit requires that the administrative interface for the GoAnyWhere server is accessible to the attacker. At the time of writing this post, X-Force detected over 700 GoAnyWhere servers available on the Internet with nearly 100 GoAnyWhere servers with the default license management ports exposed.



As detailed by security researcher, frycos, a payload to exploit the vulnerability can be created using ysoserial and the hardcoded secret keys. Ysoserial, created by frohoff, is a collection of utilities discovered in common java libraries that can exploit Java applications vulnerable to unsafe deserialization of objects.







Detection Opportunity Via Process Execution

Invoking Process = <GoAnyWhereInstallDir>/GoAnywhere/jre/bin/java

Process Name = command interpreters or LOLBins (cmd.exe, powershell.exe, certutil.exe, wmic.exe, whoami.exe, python, perl, bash, whoami, etc.)

Detection Opportunity Via Log Monitoring

Log file = %GoAnyWhereInstallDir%\userdata\logs\goanywhere.log

String Match = “request URI ‘/goanywhere/lic/accept/’ from ip address” AND “HTTP status code is ‘500’”

Detection Opportunity Via Network Traffic

POST or GET to URI “<MFTServer>/goanywhere/lic/accept?bundle=” and URI contains “bundle=” FROM Untrusted Hosts

Threat Driven Approach to Zero Days

During this incident, the time between the security advisory and the exploitation of CVE-2023-0669 was less than 1 day making it one of the fastest adoption time frames by finically motivated attackers observed by X-Force since 2020. The X-Force Vulnerability and Exploit Database, which has been curating vulnerability and exploit data since 1993 shows that the number of zero days released is increasing year over year, but X-Force observes just a handful of zero days rapidly adopted by cyber criminals each year. It begs to question, “why are some zero days rapidly and widely adopted for criminal operations and others not?”. Based on the data from the X-Force database and incident response engagements, it appears that that not every zero day is created equal. While every zero day is important and organizations should still devote efforts to patching zero days once a patch is released, there are characteristics of certain zero days that make them more likely to be rapidly and widely adopted by cyber criminals.

The following CVEs were the most rapidly and widely adopted zero days by cyber criminals observed by X-Force since 2020:

- CVE-2020-1472 (ZeroLogon)
- CVE-2021-26855 (ProxyLogon)
- CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 (ProxyShell)
- CVE-2021-34527 (PrintNightmare)
- CVE-2022-26925 (PetitPotam)
- CVE-2023-0669 (GoAnyWhere)

In 2021 X-Force released a blog detailing “How Ransomware Attacks Happen” and it turns out that the attack path detailed in that post has a direct relationship with zero day adoption by cyber criminals. Analyzing the most widely used zero days, what an attacker can achieve through exploitation, and the incidents in which they were used, indicates that the zero days that enable ransomware operators to quickly and easily obtain their goals and objectives are more likely to be used “in the wild”.

ZeroLogon — Allows an unauthenticated attacker with network access to a domain controller to exploit a NetLogon session and gain domain administrator privilege.

PrintNightmare — Is a vulnerability affecting the Windows Print Spooler service that enables an attacker to escalate privileges either locally or remotely by loading a malicious DLL which will be executed as SYSTEM.

PetitPotam — Is a NTLM relay attack that allows a remote, unauthenticated attacker to take control of an Active Directory domain by triggering a domain controller to relay its credentials to a system controlled by the attacker. With the domain controller NTLM credentials, the attacker can relay them to Active Directory Certificate Services (AD CS) to obtain a DC certificate. The attacker can use the DC certificate request a TGT (Ticket Granting Ticket) and take control of the entire domain through Pass-The-Ticket attacks.

Because ZeroLogon, PrintNightmare, and PetitPotam allow an attacker to obtain privileged access to Active Directory without credential harvesting or lateral movement, it significantly simplifies the ransomware attack path and as such X-Force observed their use on multiple ransomware attacks.

ProxyShell and ProxyLogon are vulnerabilities that affect on-premises Microsoft Exchange that enable a remote attacker to elevate privileges and execute arbitrary commands on vulnerable servers. Microsoft Exchange is an attractive target for attackers because they host business email which can enable internal phishing as well as but also given the tight integration between Exchange and Active Directory, it can also be exploited to move laterally to other high-value systems or access privileged account credentials. According to Microsoft, "If compromised, Exchange servers provide a unique environment that could allow attackers to perform various tasks using the same built-in tools or scripts that admins use for maintenance."

X-Force has observed ProxyShell and ProxyLogon leveraged in multiple ransomware attacks where the attacker was able to obtain domain administrator privileges, exfiltrate sensitive business data, and deploy ransomware directly from the Exchange servers.

Regarding GoAnyWhere, X-Force's observations are that the servers that are exploited tend to be domain-joined Microsoft Windows system that enable the attacker to immediately obtain an opportunity to gain access to high-value systems within Active Directory.

A notable absentee from the widely adopted zero-day list was Log4J. While Log4J gained widespread media attention, X-Force did not respond to many serious finically motivated incidents where Log4J was exploited. It is possible that organizations did a heroic job of patching vulnerable systems, however, given the number of systems still vulnerable to CVE-2021-44228 it appears that cyber criminals have not adopted it as widely for another reason. One interesting data point that may explain why Log4J has not been observed in as many incident response engagements is that based on X-Force vulnerability data, the majority of vulnerable Log4J systems are running Linux. Pivoting from Linux to Microsoft Active Directory requires more knowledge, capabilities and falls outside of the normal ransomware attack lifecycle further indicating that the ransomware attack lifecycle is driving zero-day adoption for cyber criminals.

A Path Forward: Understanding the Attackers

The path forward for zero-day preparation and management requires organizations adopt a threat driven approach. It's critical that organizations understand which attackers are most likely going to target them, what the attackers' goals and objectives are, and how the attackers going about accomplishing them. With this knowledge, organizations will be better prepared to identify which vulnerabilities and zero days are most likely going to be adopted. But prevention alone is no longer enough. It's equally important today to focus on detection

engineering – finding new ways to lengthen attack lifecycles and making it harder for threat actors to execute their objectives. By improving detection and response capabilities, businesses can make it more difficult for attackers to complete their goals even if they are able to gain access through vulnerability exploitation.

IBM X-Force

If you are interested in learning more about detection and response, vulnerability management, or threat hunting, X-Force provides world class proactive and reactive services to ensure your organization achieves complete preparedness for zero-day attacks. To learn how IBM X-Force can help you with anything regarding cybersecurity including incident response, threat intelligence, or offensive security services schedule a follow up meeting here:

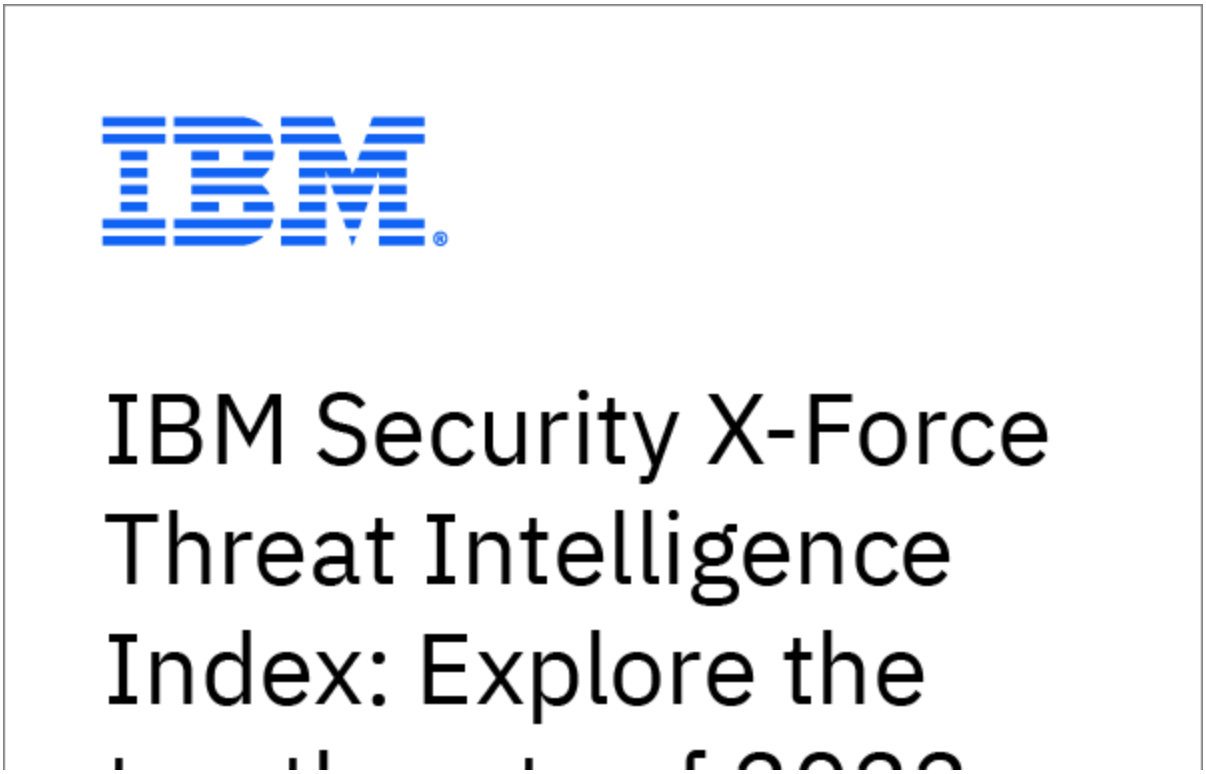
IBM X-Force Scheduler

If you are experiencing cybersecurity issues or an incident, contact X-Force to help:

US hotline 1-888-241-9812 Global hotline (+001) 312-212-8034.

Endpoint | Incident Response
John Dwyer
Head of Research, IBM Security X-Force

John (@TactiKoolSec) is the Head of Research for the IBM Security X-Force where he leads research efforts to understand and model adversary operations, devel...



top threats of 2022.

Read the report →