



Cybersecurity Threat Trends

André Murphy, Federal CTO

CAPT André Murphy, USCG (Ret), CISSP, CISM, CCSP



Federal CTO, CrowdStrike



<https://linkedin.com/in/andre-murphy>

- As the Federal CTO, lead strategic initiatives & support product direction to aid FCEB, DoD and IC partners in their cyber objectives
- Retired as a CAPT after 26 years in the U. S. Coast Guard, finishing career as the Senior Information Security Officer
 - Developed strategic cybersecurity policies & standards to manage enterprise information security risk and mature the services information security program
- Previously served as the Information System Owner and Program Manager for the Coast Guard's Combat Management System
- Managed Incident Response in Ports of NY/NJ & Delaware Bay
- Del Bay Area Maritime Security Committee's Cyber Subcommittee





2023 GLOBAL THREAT REPORT



NOWHERE TO HIDE

CROWDSTRIKE
2023
THREAT
HUNTING
REPORT



2022 Themes

- eCrime actors gained notoriety for high-profile attacks
- Dominating the espionage landscape: China-nexus adversaries significantly increased 2022 operational scale

2023 Themes

- Identity threats have become mainstream
- Adversaries are getting smarter in the cloud
- eCrime is surging as adversaries become faster





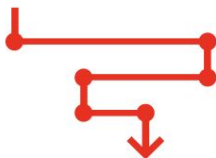
eCRIME BREAKOUT TIME

79'

**Initial
Access**



**Lateral
Movement**



Every Second Counts



Minimize cost and damage

To contain the threat, defenders must respond within the breakout time



Adversaries are getting faster

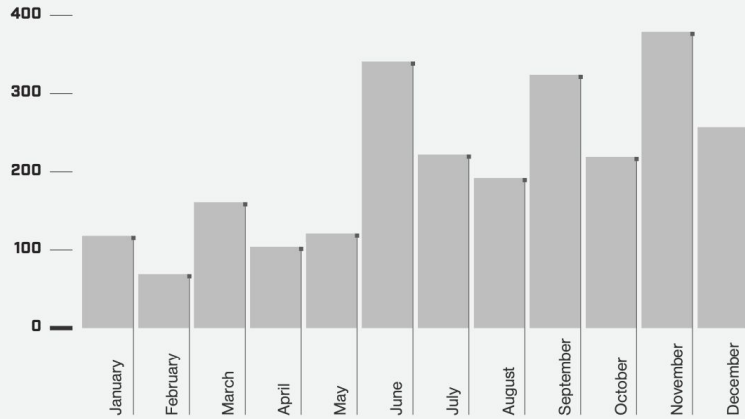
Adversaries have gotten 5 minutes faster. Have you?



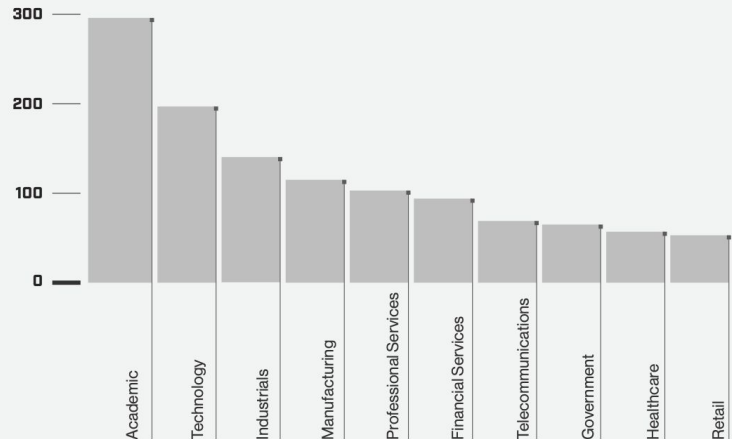
7 Min fastest breakout time

Are you equipped to face the most proficient adversaries with 7 minutes?

ACCESS BROKER ADVERTISEMENTS BY MONTH, 2022



TOP 10 SECTORS ADVERTISED BY ACCESS BROKERS, 2022



Access Broker Boom



Acceleration of demand

Popularity of services increasing with more than 2,500 advertisements –
In 2022, there was a 112% increase from 2021
In 2023, there that number rose to 147%.



Buy a la carte or in bulk

Several brokers will sell in bulk as others will use a “one-access, one-auction” technique.



Access methods remain consistent

Abuse of compromised credentials obtained by information stealers or purchased in log shops on the dark web

“ 80% of all breaches use compromised identities and 50% of organizations have experienced an Active Directory (AD) attack in the last two years. ”

Adversaries Continued to Move Beyond Malware to Gain Initial Access and Persistence

There was a continued shift away from malware use, with malware-free activity accounting for 71% of all detections in 2022 (up from 62% in 2021). This was partly related to adversaries' prolific abuse of valid credentials to facilitate access and persistence in victim environments. Another contributing factor was the rate at which new vulnerabilities were disclosed and the speed with which adversaries were able to operationalize exploits.

ADVERSARY TACTICS ■ Malware-Free

71% 2022

62% 2021

51% 2020

40% 2019

39% 2018



BEYOND USERNAMES AND PASSWORDS

Username and password or PIN

Smart card and PIN

Valid account and Active Directory certificates

APIs and secret keys

Identity providers and protocols such as SAML and OAuth

Session-based authentication, cookie-based authentication and JSON Web Tokens (JWT)

Kerberos and Kerberos tickets

Biometrics such as facial recognition, voice recognition, fingerprint recognition

Hardware and software tokens or time-based one-time password (TOTP)

Identity threats have become mainstream



Doubling down on identity intrusions

583% increase in Kerberoasting, a growing identity-based attack technique

62% of interactive intrusions involved stolen credentials



Beyond usernames and passwords

Common methods include smart card/PIN, valid accounts/Active Directory certificates, and APIs/secret keys

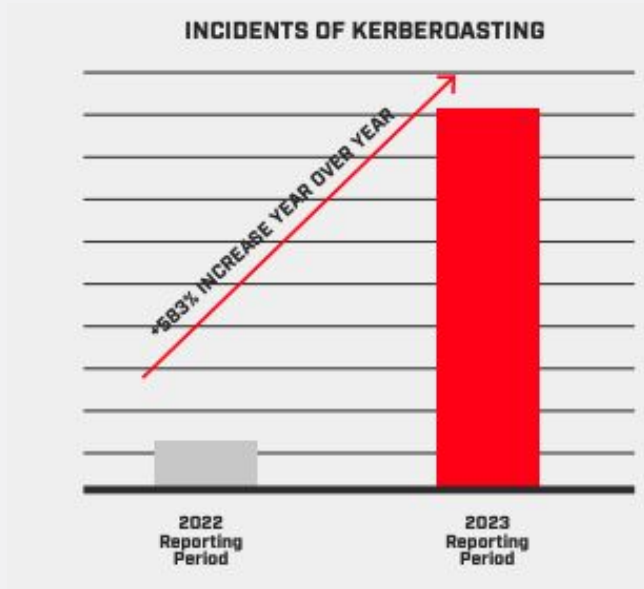


Boom in access broker advertisements

147% increase on the dark web, most notable by PROPHET SPIDER

583%

Increase in Kerberoasting, a growing identity-based attack technique



Kerberoasting Identity Attacks Skyrocketed



Proving an adversary favorite

Due to increased availability of tooling and guidance, Kerberoasting has increased drastically in popularity among eCrime adversaries



Significant threat to organizations

Adversaries do not need elevated privileges to execute this attack



VICE SPIDER

Responsible for 27% of all intrusions that involved the Kerberoasting technique

eCrime is surging as adversaries become faster



Rampant abuse of remote management tools

Illustrates adversaries' attempts to use administrative tooling to blend into enterprise noise and avoid detection



Opportunistic turns tailored TTPs

INDRIK SPIDER fluidly transitions from opportunistic initial access activity to tailored follow-on TTPs upon identifying lucrative victims



Exploit vulnerabilities for initial access

20% of all interactive intrusions involved exploitation of public-facing applications

300+%

INCREASE IN ADVERSARY USE OF RMM TOOLS YEAR OVER YEAR

147%

INCREASE IN ACCESS BROKER ADVERTISEMENTS IN CRIMINAL OR UNDERGROUND COMMUNITIES¹⁶

China-nexus adversaries significantly increased 2022 operational scale



Exploits to gain initial access

China-Nexus Adversaries continued shifting toward exploitation of web-facing services



Increase in use of zero-day exploits

Enterprise software continued to be a high-priority target. Additional zero-day exploits include weaponized MSFT Office documents.



Target Taiwan

Adversaries growing more confident leveraging traditional endpoints to pivot to cloud – and vice-versa



Zero-day exploits were most commonly observed in intrusions targeting North American organizations in 2022; China-nexus adversaries used zero-day exploits to compromise entities in the aerospace, legal and academic sectors.



“ China-nexus adversaries were observed targeting nearly all 39 global industry sectors and 20 geographic regions CrowdStrike Intelligence tracks. ”





Maritime Threats

- Advancing modernization in maritime operations increases attack surface
- Adversary **exploitation of identities** continues to grow
- Access brokers gain access via **compromised credentials** & brute-force
- Big Game Hunting (BGH) ops continue to rely on ransomware & data theft
- Internet-facing networks are ripe targets for BGH ransomware campaigns
 - Also leveraged by APTs such as China-Nexus adversaries
 - GTR case study on CrowdStrike thwarting an Ethereal Panda attack by Web Service
- > **59 Cybersecurity Reports** in US maritime sector in 2022; **13 ransomware**
- Thetius, CyberOwl & HFW research shows avg ransom payment - **\$3.2M**



Energy Threats

- **Ransomware & data extortion** ops still lucrative for eCrime adversaries
 - BITWISE SPIDER's LockBit RaaS - most prolific BGH operation in 2022
 - BITWISE SPIDER's LockBit 3.0 - most energy ransomware ops MAR22-MAR23.
- MAR22-MAR23 CRWD Intel ID'd **68 ransomware** energy sector incidents; > 25 US
- **\$4.82M** - 2022 avg critical infrastructure data breach - Ponemon Institute & IBM Security
 - 14SEP22, the U.S. government levied sanctions against individuals & orgs associated w/ NEMESIS KITTEN for data extortion & ransomware
 - **2 critical infrastructure orgs**, regional electric utility companies (MS & IN)
- Access brokers advertised for energy sector entities
- Espionage: China-nexus adversaries most likely threat
- eCrime: (BGH) operations likely to remain the most significant threat



Notable Maritime Incidents

Up to 1,000 ships affected by DNV ransomware attack

Ransomware

Adis Ajdin · January 13, 2023

Three Canadian ports hit by cyber attacks

Denial of Service

Kim Biggar · April 13, 2023

Aker Solutions' Brazilian subsidiary CSE hit by cyber attack

Ransomware

Adis Ajdin · February 15, 2023

The Largest Ferry Service from Massachusetts Hit by a Ransomware Attack

Authority Was hit by a Ransomware Attack Which Led to Ticketing and Disruptions.

Ransomware

UPDATED ON JUNE 4, 2021

PORT OF HOUSTON WAS HIT BY AN ALLEGED STATE-SPONSORED ATTACK

APT

Pierluigi Paganini · September 26, 2021

Cyberattack Threatens Release of Port of Lisbon Data

Ransomware

PUBLISHED DEC 29, 2022 6:34 PM BY THE MARITIME EXECUTIVE





5 Steps To Be Prepared

1 Gain visibility into your security gaps

2 Prioritize identity protection

3 Prioritize cloud protection

4 Know your adversary

5 Practice makes perfect

Identity Protection Example & AI Summary

Charlotte AI Investigator

Incident level summary

Charlotte AI Investigator
Oct. 23, 2023 23:00:57

Charlotte AI Investigator identified suspicious RDP activity from known compromised host XDR-STH-WIN10-1 to host XDR-STH-WIN10-5 on September 17th, 18:46 UTC. AI Investigator observed additional suspect RDP activity from XDR-WIN10-1 to XDR-STH-WIN10-7 on September 17th, 18:57 UTC.

[Add to notes](#)

Suggestions [Accept all suggestions](#)

XDR-STH-WIN10-3 [Preview](#)

OS	External IP Address	Host ID
Windows 10	172.17.0.30	9b7e3837ee924d5dcb...

Users: ddursley (managed, compromised 2023-09-17 04:19:16)

[Dismiss](#) [Accept suggestion](#)

XDR-STH-WIN10-1 [Preview](#)

OS	External IP Address	Host ID
Windows 10	172.17.0.26	aeb77fb5103d4b6899...

Users: ddursley (managed, compromised 2023-09-17 04:21:50)

[Dismiss](#) [Accept suggestion](#)

20.121.51.80 [Preview](#)

OS	External IP Address	Host ID
Windows 10	20.121.51.60	unknown

Users: ddursley (unmanaged, compromised 2023-09-17 04:39:29)

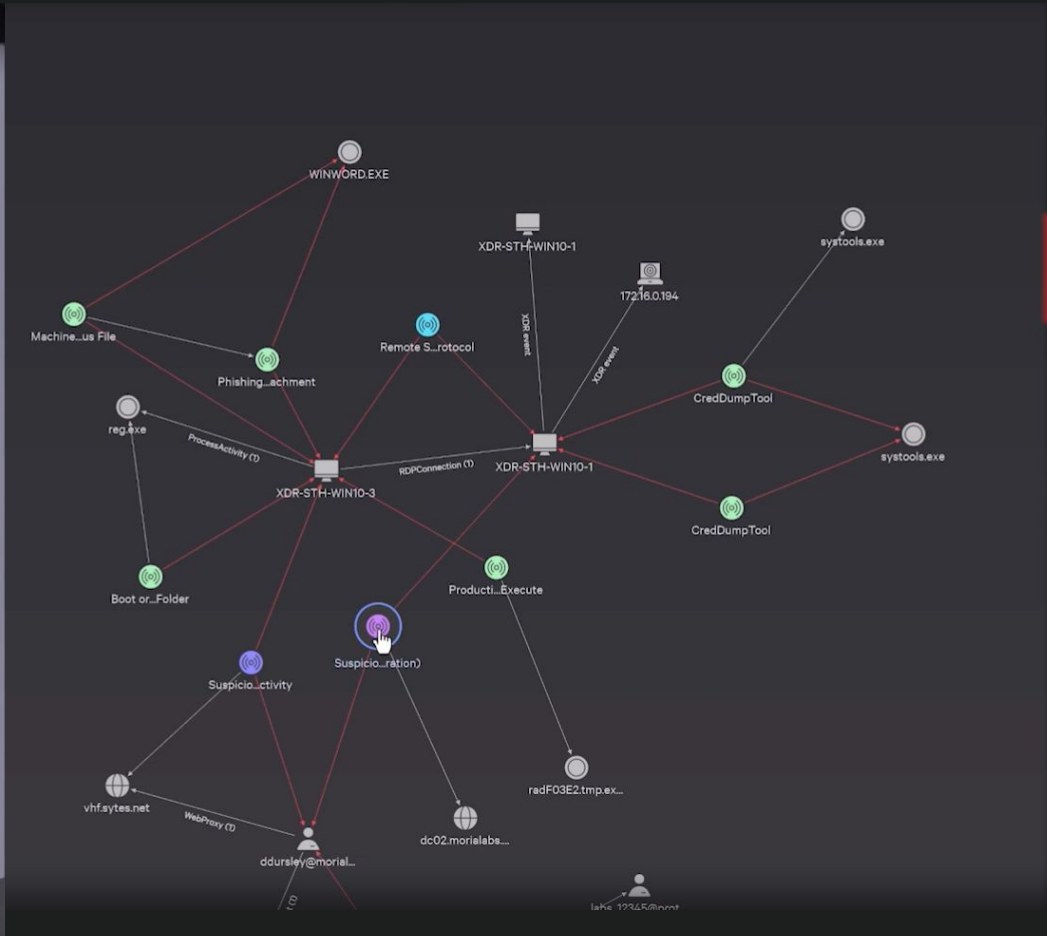
[Dismiss](#) [Accept suggestion](#)

172.16.0.10 [Preview](#)

OS	External IP Address	Host ID
Windows 10	172.16.0.10	unknown

Users: ddursley (unmanaged, compromised 2023-09-17 04:39:29)

[Dismiss](#) [Accept suggestion](#)



Suspicious LDAP search (Kerberos misconfiguration)

Identity indicator

Credential Access via Steal or Forge Kerberos Tickets

Event time: Sep. 24, 2023 21:00:08 | Log source: CrowdStrike

Tactic & technique: Credential Access via Steal or Forge Kerberos Tickets

Domain: **Identity**

Description: A user executed a suspicious LDAP search looking for Kerberos misconfigurations

Related IDP detection: [Detection](#) | Source host name: xdr-sth-win10-1.morialabs.com

[Show all](#) | [See event details](#)

Contextual behaviors

Find them. Know them. Stop them.

Discover the adversaries targeting your industry.

- Adversaries
- Threat Report
- eCrime Index

Your Industry: Business Size: Your Country:

Your Threat Landscape [Back to Global Threat Landscape](#)



Adversaries potentially targeting you **7 of 225**

[View recommended solution](#)

Veto Spider	Hive Spider	Cosmic Wolf	Banished Kitten	Vapor Panda	Royal Spider	Lunar Spider
Wandering Spider	Partisan Jackal	Percussion Spider	Haywire Kitten	Sunrise Panda	Brain Spider	Clockwork Spider
Recess Spider	Vice Spider	Thunderbolt Jackal	Nemesis Kitten	Phantom Panda	Hermit Spider	Sally Spider
Lily Spider	Bitwise Spider	Frontline Jackal	Frontline Kitten	Empire Bear	Gossamer Bear	Mummy Spider
Shrub Spider	Developer Spider	Forest Kitten	Frontline Kitten	Empire Bear	Empire Bear	Indrik Spider
Holly Spider	Scattered Spider	Sortie Spider	Eastern Europe	Smoky Spider	Smoky Spider	Cozy Bear
Scattered Spider	Sortie Spider	Sortie Spider	Eastern Europe	Smoky Spider	Smoky Spider	Woodoo Bear
Mirage Tiger			Eastern Europe	Smoky Spider	Smoky Spider	Berserk Bear

Explore the Adversary Universe

Get your personal threat landscape

<https://www.crowdstrike.com/adversaries/>



Resources

- 2023 Global Threat Report - <https://www.crowdstrike.com/global-threat-report/>
- 2023 Threat Hunting Report - <https://www.crowdstrike.com/resources/reports/threat-hunting-report/>
- Adversary Universe - <https://www.crowdstrike.com/adversaries/>
- Adversary Universe Podcast - <https://www.crowdstrike.com/resources/adversary-universe-podcast/>
- Port Security Grant Program - <https://www.fema.gov/grants/preparedness/port-security>
- CrowdStrike Detects and prevents Labyrinth Chollima Supply Chain Attack - [Link](#)
- Identity Protection against Kerberoasting attacks & Charlotte AI incident summary - [Link \(video\)](#)
- Attack and Defend Demo using Identity Threat Protection - [Link \(video\)](#)



A stylized, monochromatic red illustration of a character in a cockpit. The character has a helmet with a red visor and a stern expression. The cockpit is filled with various mechanical details and a steering wheel. At the bottom center, there is a globe. The entire scene is rendered in shades of red and dark red, with a halftone dot pattern in the background.

Questions?