
cisco Live!
Let's go

The bridge to possible

Catalytic Converter Theft

Or what happens when you focus on just the #1 Threat

Thorsten Rosendahl
@MjolnirOperator

What this session is about and what not

- Catalytic Converter theft is just an analogy
  I will deliver to the headline for 5 minutes
- We wont be taking a single/specific malware apart
- I will not be talking about cisco products or their configuration

- We will be walking through analyzed telemetry from 2023

I do not have a crystal ball ...if you want to talk about 2024,

I need a 5 star rating and we meet here next year

Who am I

- 27 years Cisco Employee
- @Talos since about 12 Months

- Love to tinker with MCU’s.
- Enjoying Offgrid and Offroad Adventures
- German – hence the relation to cars and catalytic converters

Talos powers the Cisco portfolio with comprehensive intelligence

Every customer environment, every event, every single day, all around the world

Catalytic Converter Theft

Across Europe (and RoW too)


Curiosità e Suggerimenti

Così eviti il furto di uno dei componenti più preziosi | Bastano pochi secondi per rubarlo

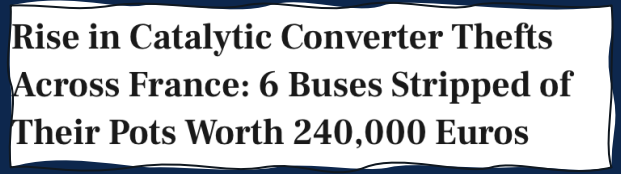
Agosto 21, 2023 Luca Papperini

https://www.autoruote4x4.com/2023/08/21/cosi-eviti-il-furto-di-uno-dei-componenti-piu-preziosi-bastano-pochi-secondi-per-rubarlo/


Katastrofal ökning: "Så här kan det inte fortsätta"

Antalet anmälda fall har ökat med 10 000 procent på två år.

https://www.mestmotor.se/automotorsport/artiklar/nyheter/20220330/ny-rapport-lavinartad-okning-av-katalysatorstolder/


Rise in Catalytic Converter Thefts Across France: 6 Buses Stripped of Their Pots Worth 240,000 Euros

https://www.world-today-news.com/rise-in-catalytic-converter-thefts-across-france-6-buses-stripped-of-their-pots-worth-240000-euros/


Catalytic converter theft skyrockets in Finland

Where the stolen catalytic converters end up is unclear.

https://yle.fi/a/74-20021345


In about three years, there have been more than 1,500 reports of catalytic converter theft in Brabant. The increase is explosive, as three years ago, there were only 70 reports of theft of the auto part. In fact, in the first three months of this year, the most stolen catalytic converters were reported in our province in the whole of the Netherlands.

https://eindhovennews.com/news/2023/06/increase-in-catalytic-converter-thefts/


Gang that stole more than 500 catalytic converters all over Spain is dismantled

Crime · The police operation - carried out in the provinces of Malaga, Madrid and Toledo - has resulted in the arrest of 29 people

https://www.surinenglish.com/spain/gang-that-stole-more-than-500-catalytic-20230322165945-nt.html

Supply Chain !

https://www.ciscolive.com/on-demand/on-demand-library.html?search=BRKSEC-2727#/

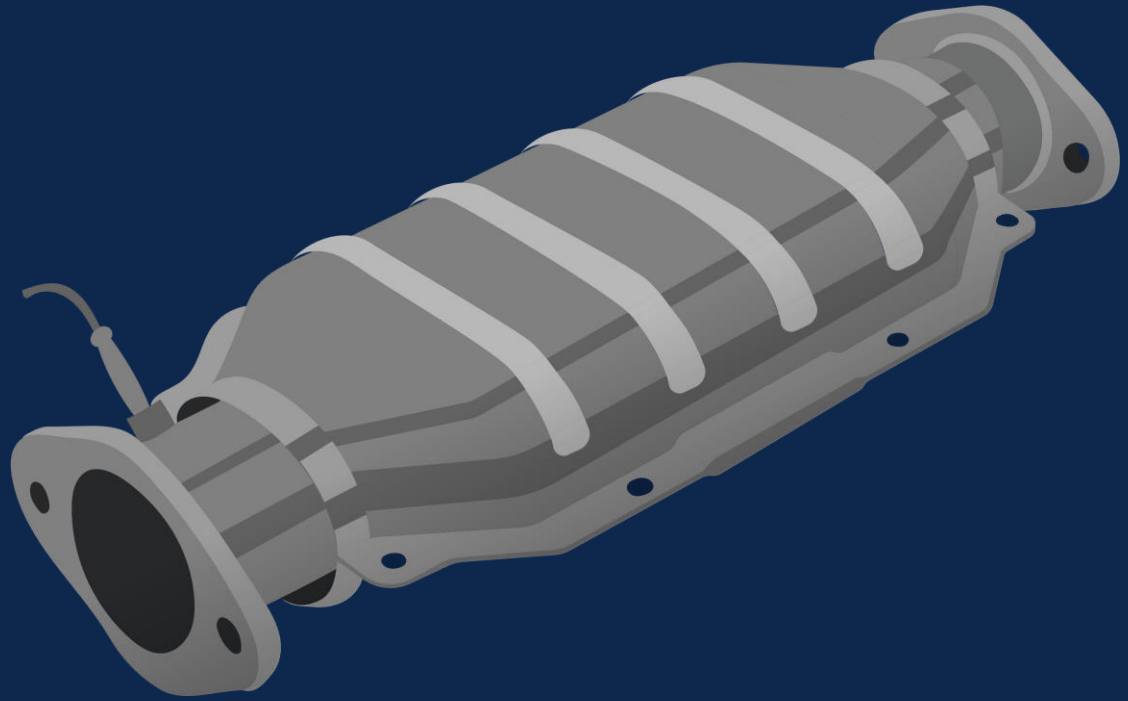
9 Jul 2023 | News

Why are Catalytic Converters a Target?

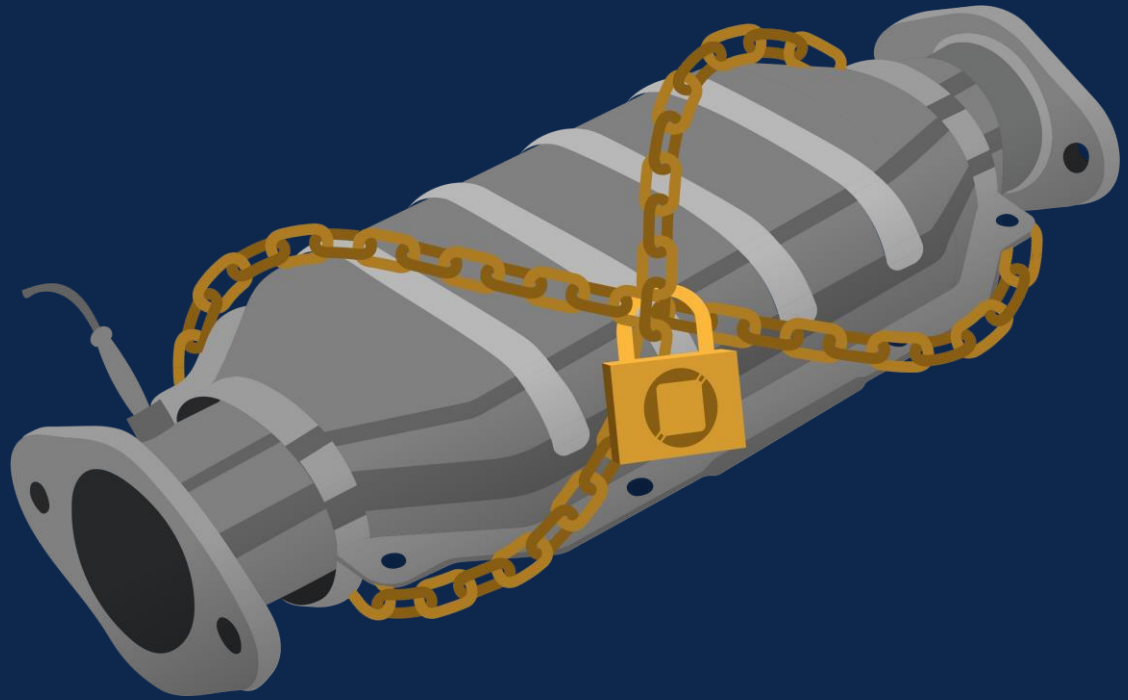
On 16 May 2023, cargo thieves attacked and hijacked a truck travelling en route from Port Elizabeth to Cape Town, South Africa. The truck driver was shot and seriously injured.

https://iapaemea.org/news/why-are-catalytic-converters-a-target/

What happens when we focus on just the #1 Threat



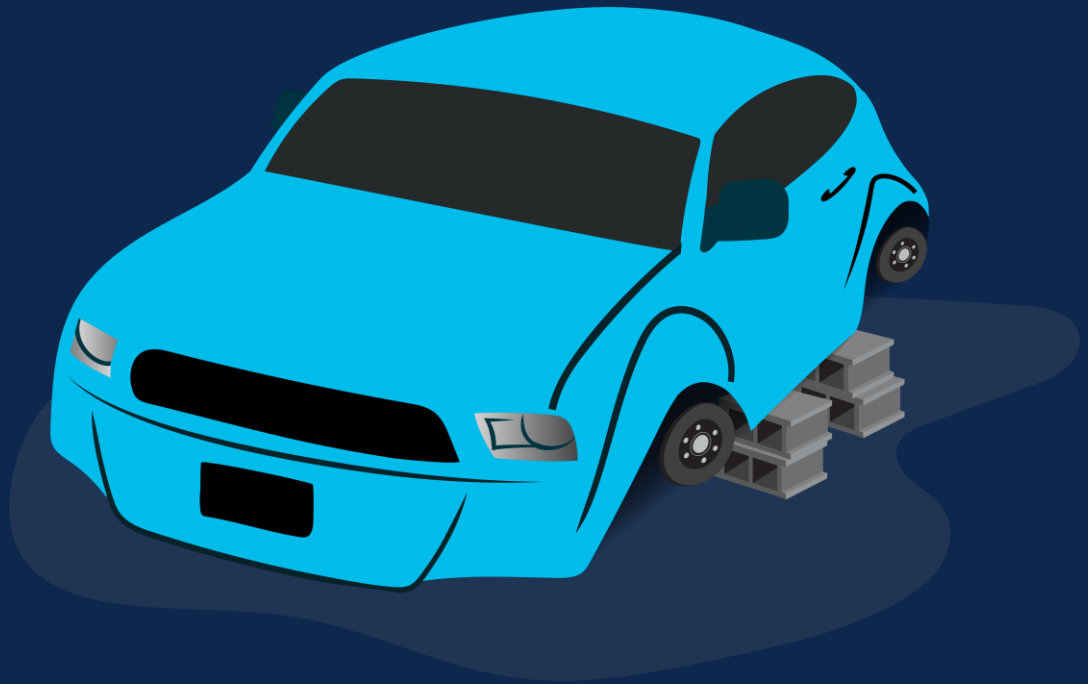
We will focus on just the No. 1 threat



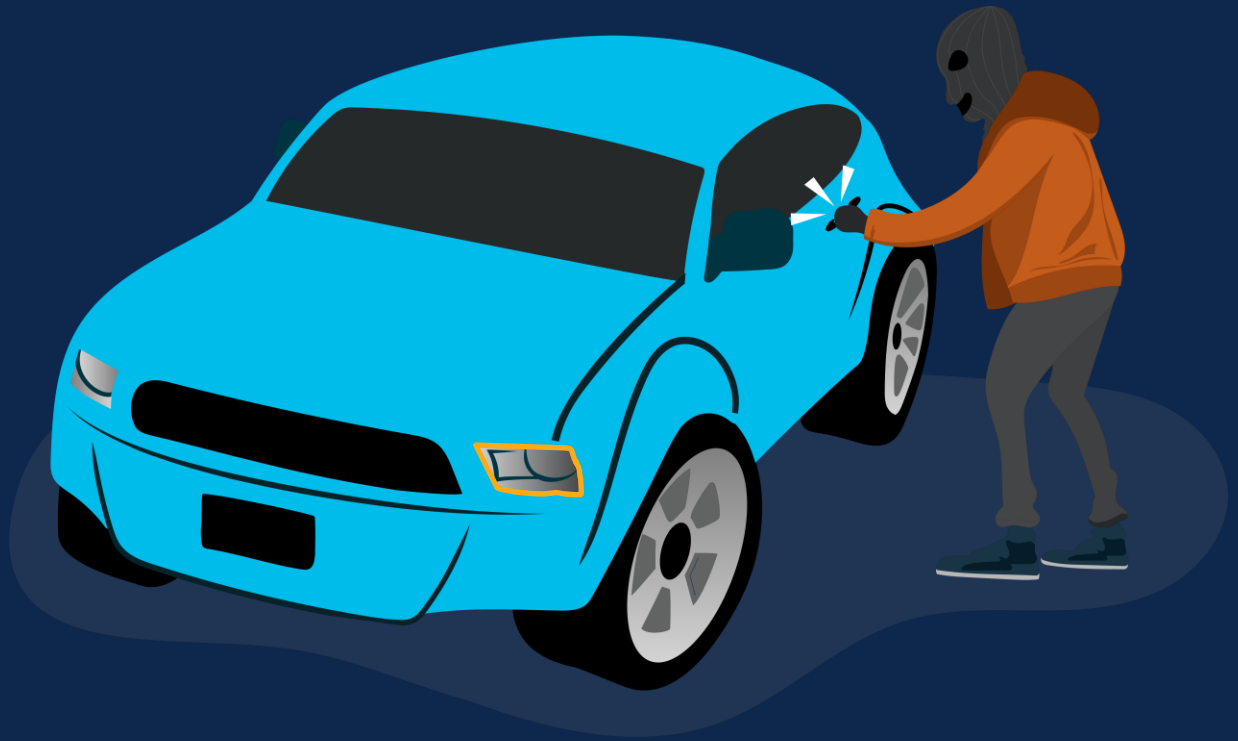
Catclamp

https://catclamp.com/

But equally important there is



And there is also that

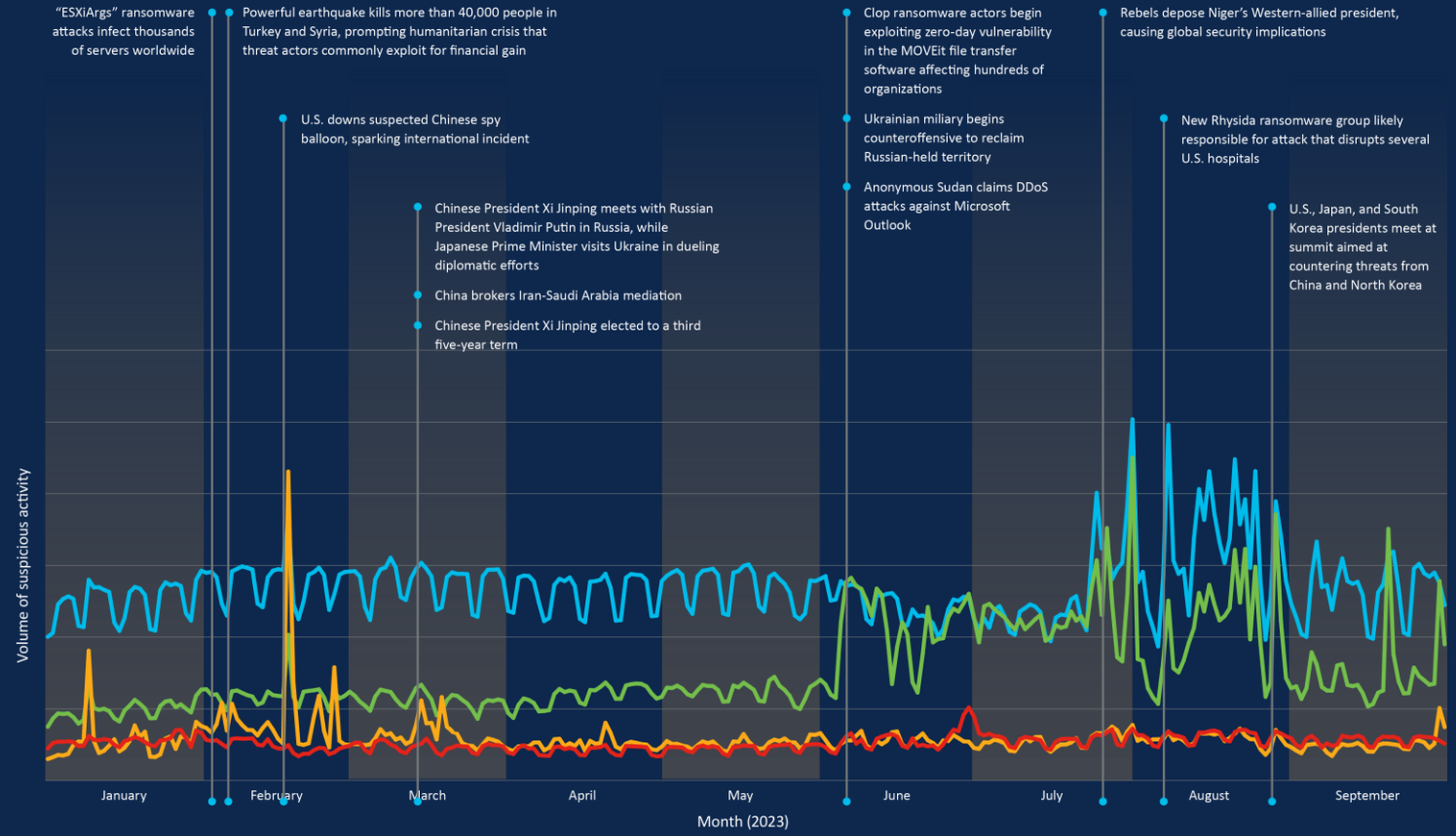


2023
A year in Review

https://blog.talosintelligence.com/cisco-talos-2023-year-in-review

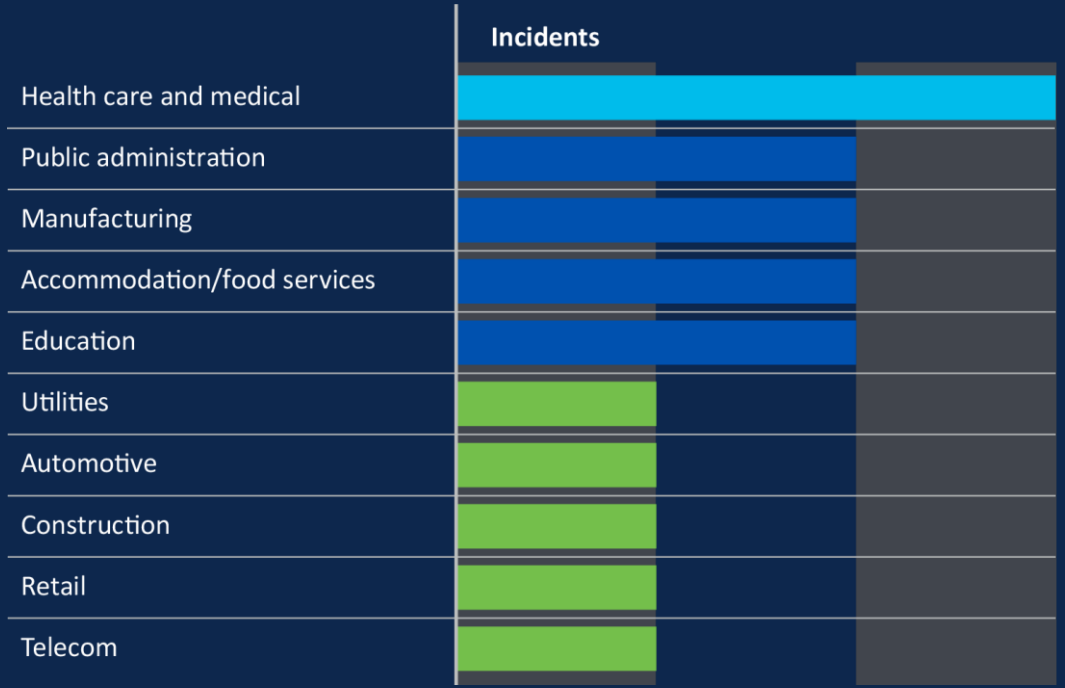
Telemetry Trends

Regional trends summary



Healthcare most targeted sector

Talos IR ransomware and pre-ransomware incidents per sector



- The health care and public health sector was the most targeted vertical in Talos IR ransomware and pre-ransomware engagements this year, compared to the education sector in 2022.

Top initial access vectors

Talos Incident Response data

Top initial access vectors

Talos Incident Response data

Update your software

Establish Logging / Analytics

MFA, MFA, MFA

Top targeted vulnerabilities

Ranking	CVE	Vendor	Product	CISA findings	CISA KEV catalog	Kenna/CVSS
1	CVE-2017-0199	Microsoft	Office and WordPad	Routinely exploited in 2022	Yes	100/9.3
2	CVE-2017-11882	Microsoft	Exchange server	Routinely exploited in 2022	Yes	100/9.3
3	CVE-2020-1472	Microsoft	Netlogon	Routinely exploited in 2022	Yes	100/9.3
4	CVE-2012-1461	Gzip file parser utility	Multiple antivirus products			58/4.3
5	CVE-2012-0158	Microsoft	Office	Commonly exploited by state-sponsored actors from China, Iran, North Korea, and Russia (2016-2019)	Yes	100/9.3

- Exploitation of older software vulnerabilities in commonly used applications
- Low cost/high impact target for threat actors

Source: Cisco Secure Endpoint
CISA sources: Top Routinely Exploited Vulnerabilities, 2022 and 2016 - 2019.

Top targeted vulnerabilities

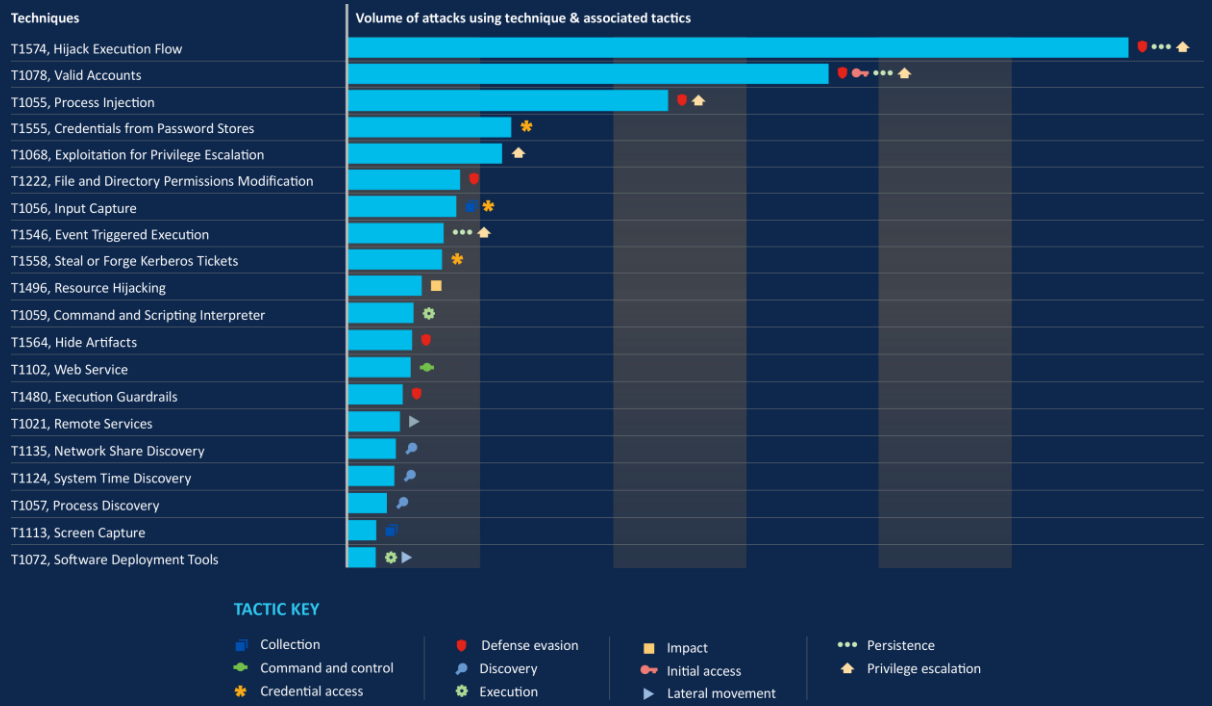
Ranking	CVE	Vendor	Product	CISA findings	CISA KEV catalog	Kenna/CVSS
1	CVE-2017-0199	Microsoft	Office and WordPad	Routinely exploited in 2022	Yes	100/9.3
2	CVE-2017-11882	Microsoft	Exchange server	Routinely exploited in 2022	Yes	100/9.3
3	CVE-2020-1472	Microsoft	Netlogon	Routinely exploited in 2022	Yes	100/9.3
4	CVE-2012-1461	Gzip file parser utility	Multiple antivirus products			58/4.3
5	CVE-2012-0158	Microsoft	Office	Commonly exploited by state-sponsored actors from China, Iran, North Korea, and Russia (2016-2019)	Yes	100/9.3

- Exploitation of older software vulnerabilities in commonly used applications
- Low cost/high impact target for threat actors

Source: Cisco Secure Endpoint
CISA sources: Top Routinely Exploited Vulnerabilities, 2022 and 2016 - 2019.

Top MITRE ATT&CK techniques

Volume of attacks using technique and associated tactics



Source: Cisco Secure Endpoint

- ~33% of top techniques fall in the defense evasion tactics
- Privilege escalation and persistence techniques also ranked highly
- Cryptocurrency mining malware used as a resource hijacking technique

Top 5 MITRE ATT&CK techniques

2023 by volume

Top 5 MITRE ATT&CK Techniques

- **41%** Hijack execution flow
- **25%** Valid accounts
- **17%** Process injection
- **9%** Credentials from password stores
- **8%** Exploitations for privilege escalation

Source: Cisco Secure Endpoint

Top 5 MITRE ATT&CK techniques
And Mitigations

Top 5 MITRE ATT&CK Techniques

41% Hijack execution flow

25% Valid accounts

17% Process injection

9% Credentials from password stores

8% Exploitations for privilege escalation

Selected MITRE ATT&CK Mitigations

M1040 Behavior Prevention on Endpoint, M1051 Update Software

M1027 Password Policies, M1032 MFA

M1040 Behavior Prevention on Endpoint

M1027 Password Policies, M1051 Update Software,
IMHO : M1032 MFA, but with Caution*
M1051 Update Software

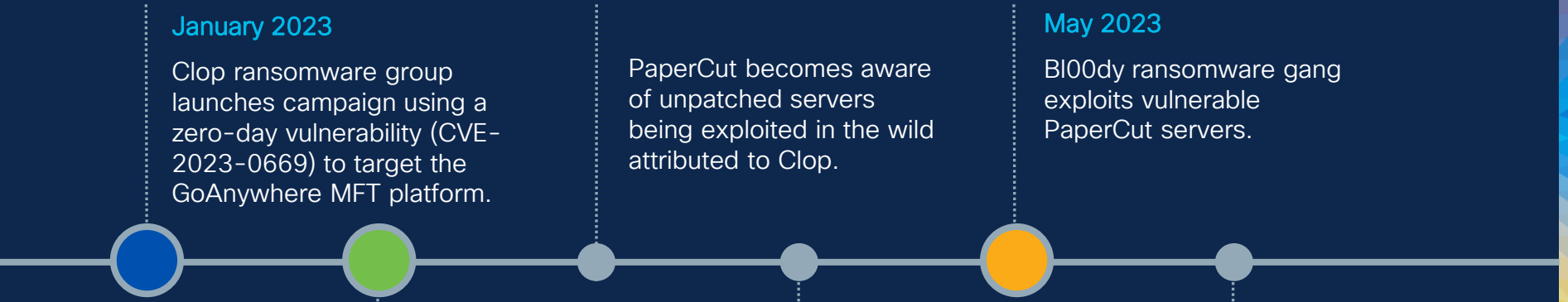
* https://blog.talosintelligence.com/what-might-authentication-attacks-look-like-in-a-phishing-resistant-future/

Ransomware and extortion

Ransom “Trends”

- We saw Clop affiliates consistently exploit zero-day vulnerabilities, a highly unusual tactic given the expertise, personnel and access required to develop such exploits, suggesting the group possesses a level of sophistication and/or resources matched only by advanced persistent threats (APTs).
- New ransomware variants are emerging that leverage leaked source code from other RaaS groups, allowing less skilled actors to enter this space
- Some groups turning into extortion

Timeline of ransomware groups leveraging notable vulnerabilities



January 2023

Clop ransomware group launches campaign using a zero-day vulnerability (CVE-2023-0669) to target the GoAnywhere MFT platform.

April 2023

Malicious actors start exploiting vulnerabilities in PaperCut (CVE-2023-27350) beginning in mid-April 2023.

PaperCut becomes aware of unpatched servers being exploited in the wild attributed to Clop.

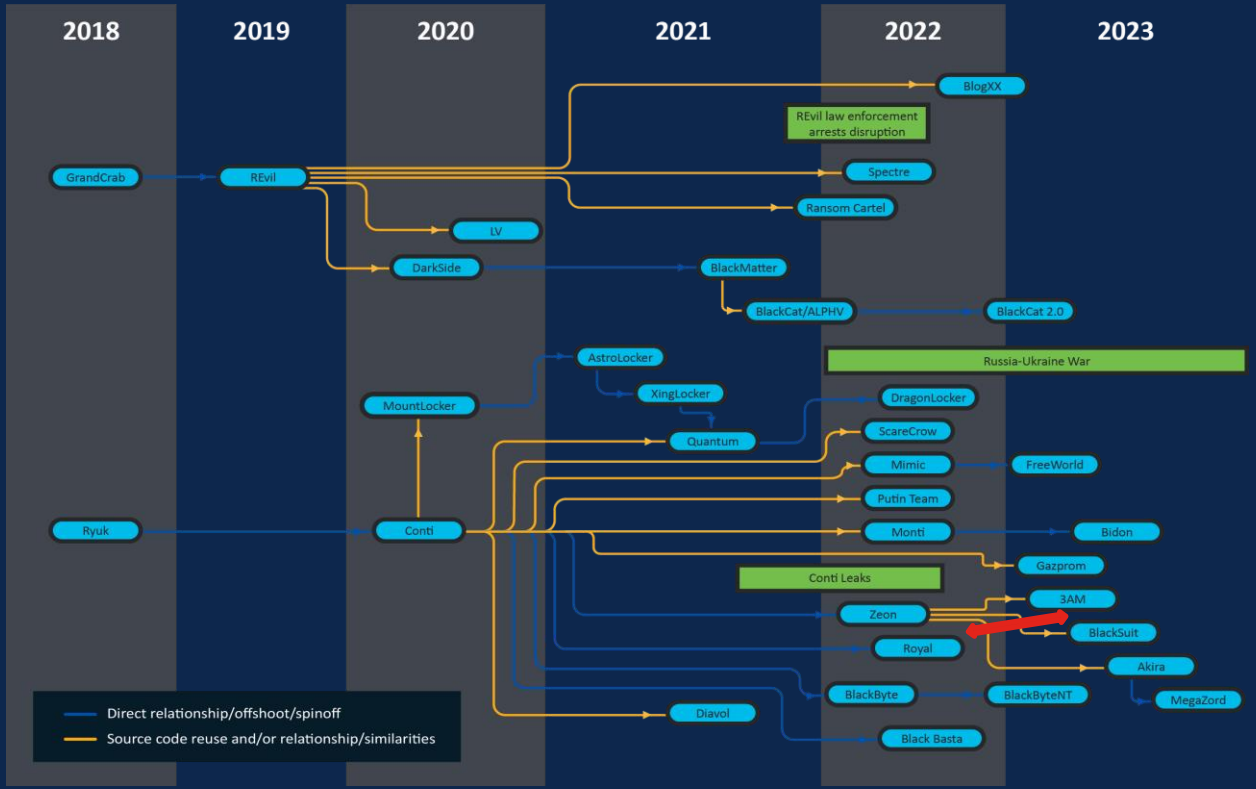
PaperCut actively exploited by malicious actors for remote code execution (RCE) to deploy LockBit ransomware.

May 2023

BI00dy ransomware gang exploits vulnerable PaperCut servers.

Clop begins exploiting a previously unknown SQL injection vulnerability (CVE-2023-34362) in Progress Software's managed file transfer (MFT) solution.

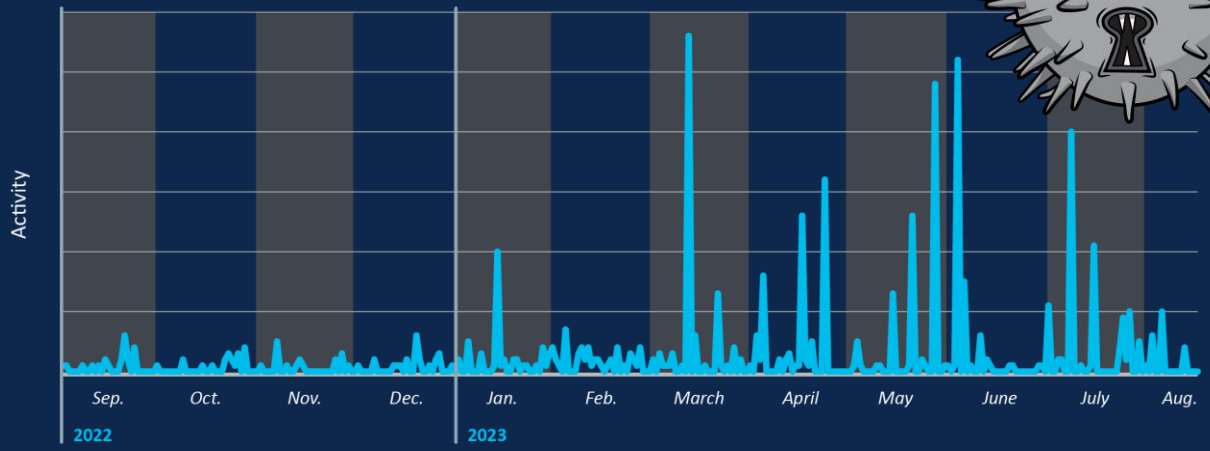
Democratization of the ransomware economy



Graphic adapted from https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map.pdf

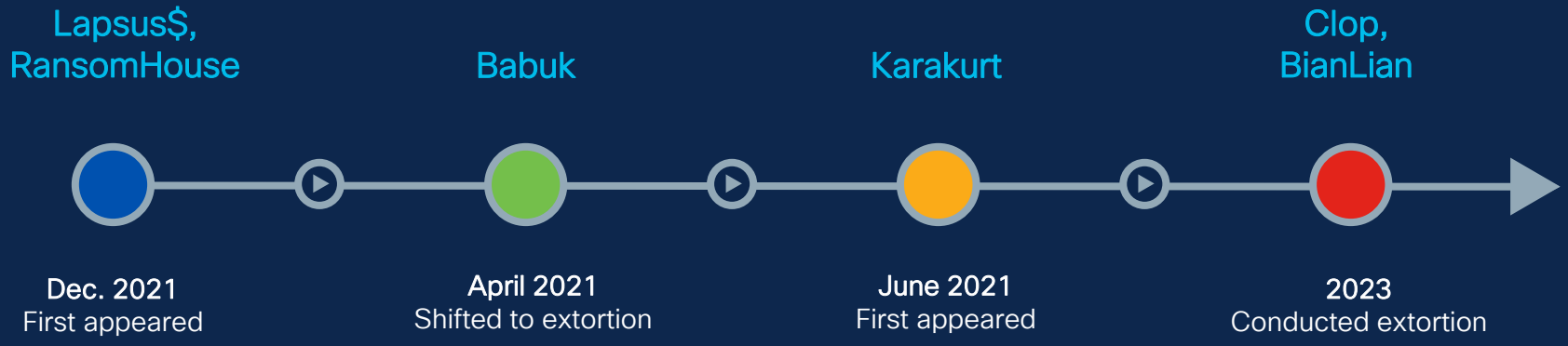
LockBit most prevalent ransomware group

- LockBit attacks can be very impactful, affecting an organization's IT networks and OT environments.
- CVE-2023-27350 spiked in March
- We also saw the ransomware affiliate gained initial access using valid router credentials



Rise over time in data theft extortion

Prominent groups increasingly turning to data theft extortion over or in addition to ransomware



Unveiling the Dutch Police's Art of Hunting Cyber Criminals - CSSSEC-1817
Wednesday, Feb 712:00 PM - 12:45 PM CET

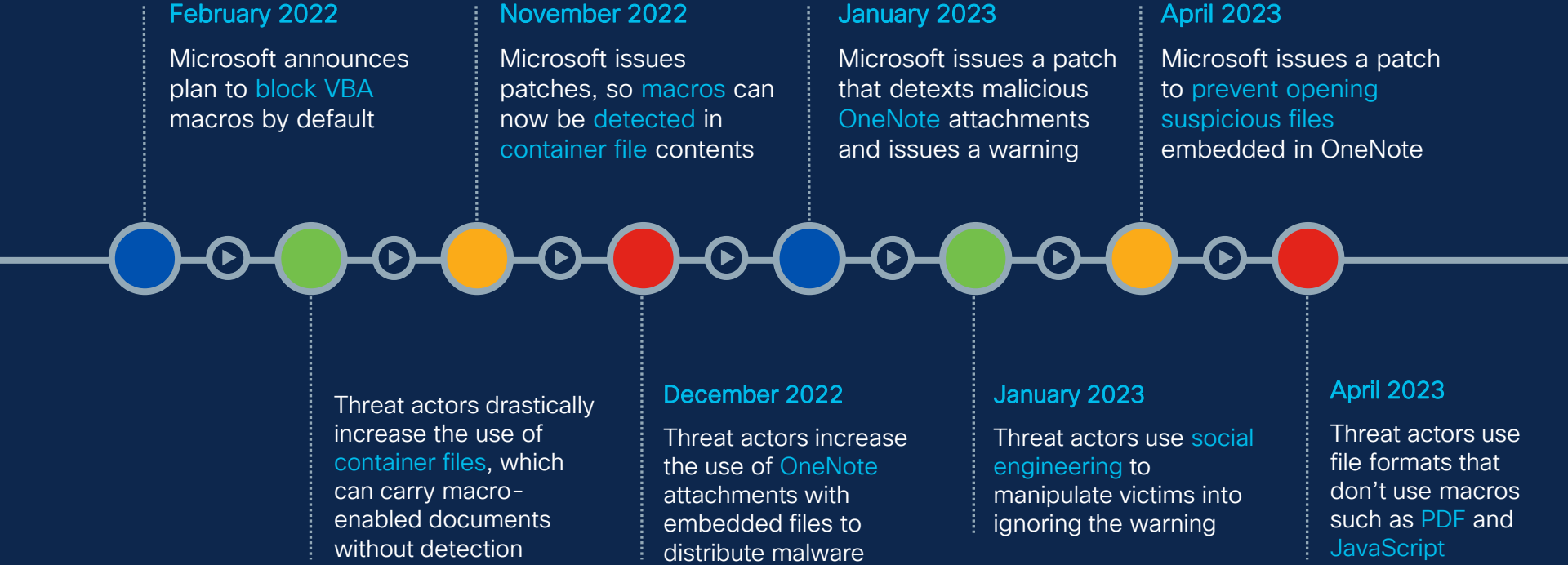
https://blog.talosintelligence.com/decryptor-babuk-tortilla/

Commodity Loaders

Commodity Loaders

- Commodity loaders such as Qakbot, Ursnif, Emotet, Trickbot and IcedID represent some of the most impactful and pervasive threats, as actors routinely rely on them to enable key parts of their operations.
- All these loaders formerly functioned solely as banking trojans, and developers have diversified their capabilities in recent years to support more advanced operations.
- Their use as downloaders for information-stealers, ransomware, and other malware have made them mainstays in the threat environment, indiscriminately affecting entities globally.

Response to new security updates blocking macros



If all else fails, stick to the old methods

While many affiliates introduced new TTPs in 2023 in response to evolving security updates, we also observed commodity loaders using older methods.

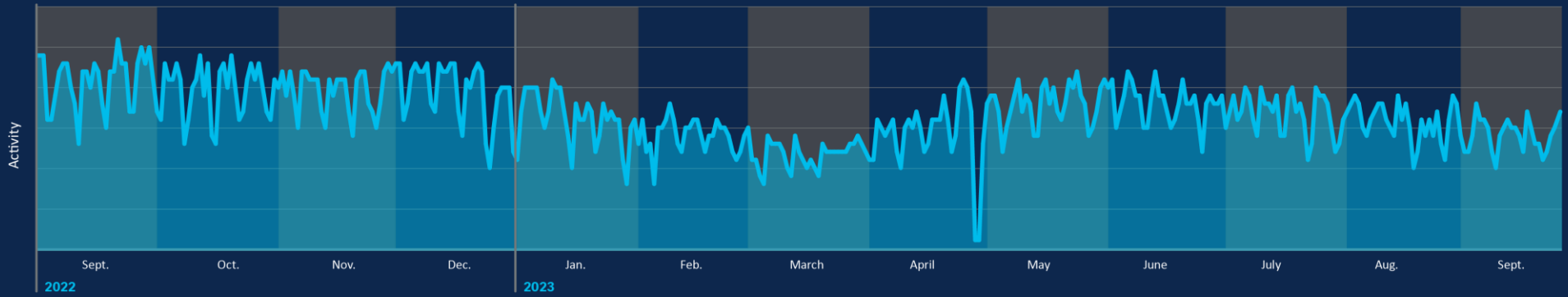
Emotet infection chain using binary padding

- Emotet, IcedID and Ursnif were all observed using macros-enabled Office documents in the initial infection chain.
- Furthermore, we observed Emotet being delivered in phishing emails with old “RedDawn” templates first seen in 2020.

Persistence long after botnets are dismantled

We have seen this from Trickbot, where Talos telemetry picked up activity throughout 2023 even though their infrastructure was dismantled in February 2022.

Trickbot activity over time



Persistence long after botnets are dismantled

- In August 2023, Qakbot was disrupted in a major global law enforcement operation, but dismantling botnet infrastructure does not always mean cybercriminals cease to operate.

https://blog.talosintelligence.com/qakbot-affiliated-actors-distribute-ransom/

Network Infrastructure

Network Infrastructure attacks

An uptick in network infrastructure attacks observed in 2023 as threat actors exploit the large attack surface and potentially vast victim network.

Advanced actors looking to advance espionage objectives and facilitate stealthy operations.

Three out of five most targeted device vulns are **highly critical or severe**

Exploitation of vulnerabilities often spike after public disclosure

Did I mention “MFA” and “update your software” today ?

APTs

Advanced Persistent Threats

While advanced persistent threats (APTs) emanating from many parts of the world remained active, most of our investigations and research focused on China, Russia and the Middle East.

APTs will take steps to weaken defenses within the environment and carve out additional paths for long-term access. These methods include disabling logging, modifying memory to reintroduce vulnerabilities that had been patched, modifying configurations to enable privileged activity and replacing firmware with older and legitimate firmware that can be modified in memory.

China

- China-linked APT groups operated at a rapid pace this year, conducting sophisticated and stealthy intrusions into the networks of numerous high-value targets.
- China-affiliated APTs appear to considerably reduce their malicious activity on a network if detected or the actor becomes aware of incident response efforts.
- We responded to several intrusions into telecommunications providers by China-affiliated APTs this year, particularly in areas that are of strategic interest to Beijing.

Russia

- Russian state-sponsored APT group Gamaredon has remained a major player in threats against Ukraine and was the top threat that the Cisco Talos Ukraine task unit responded to this year.
- Turla, another Russian government-affiliated APT group, was largely active between September 2022 and February 2023, but their operations diminished significantly around May 2023.
- We also observed a spike in SmokeLoader activity in late April and early May, aligning with CERT-UA's reporting of mass distribution of SmokeLoader targeting Ukrainian entities.

Middle East

- Events in early October 2023 between Hamas and Israel contributed to several politically motivated hacktivist groups launching uncoordinated and mostly unsophisticated attacks against both sides, like what we observed at the beginning of the Russia-Ukraine war.
- The Middle East's complicated geopolitical environment continued to be dynamic this year, and we will likely see that impact the cyber realm going forward.
- Discovery of a new actor we named ShroudedSnooper that appears intent on targeting major telecommunications entities in the region

A look ahead...

Actors

The lines are becoming blurred
Criminals will increase frequency and enhance sophistication
APTs, whether it be political, economical or military will grow in volume

TTPs

If all else fails, stick to the old methods

TTPs going forward

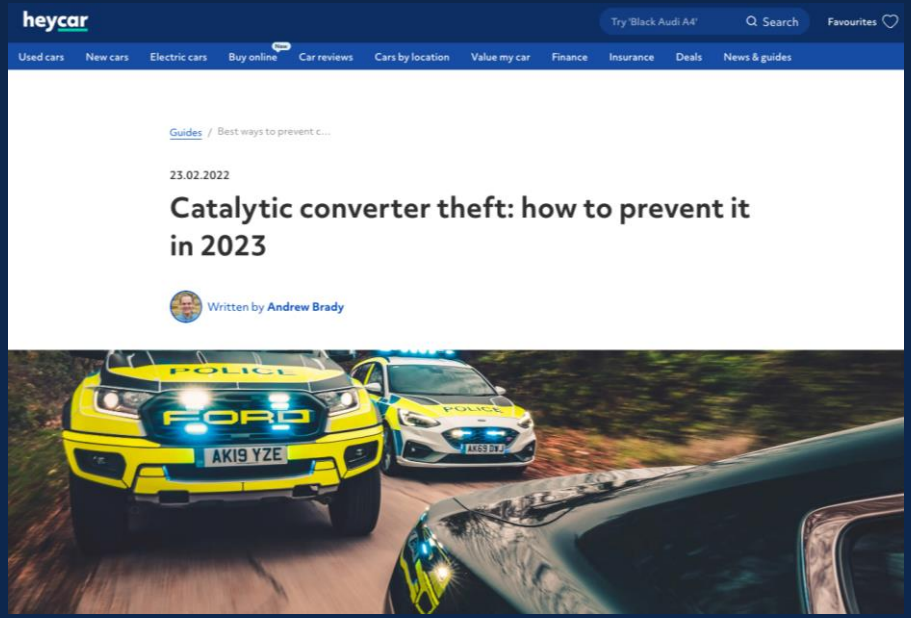
If all else fails, stick to the old methods

- Identity related attacks
  - Credentials, Keys, Cookies, Tickets
- AI powered attacks
  - Technology will mature and easier to be used for malicous purposes like social engineering, fraud, misinformation.
- Supply Chain attacks
  - A fortune 500 Company will have better controls in place than a Mom and Pop business

Targets

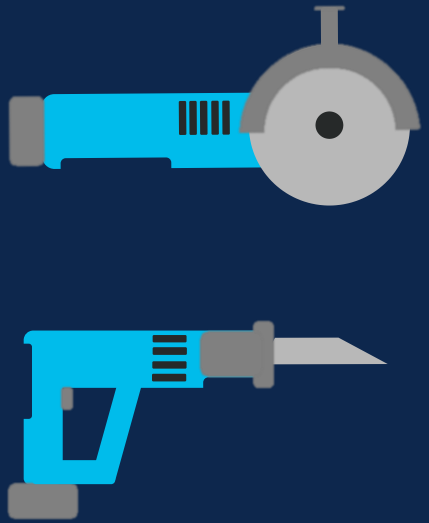
- Network Infrastructure Attacks – We just saw the beginning
- Cloud : bigger bargain if breached
- IoT : exponential (?) growth, harder to patch
- Critical Infrastructure Attacks : power grids, transportation, medical

In case you are still interested



https://heycar.co.uk/guides/best-ways-to-prevent-catalytic-converter-theft

A last word about “attribution”




cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go