PRO CISO®

Cyber Security insights
November 2022

https://prociso.com – LinkedIn - AaaSK@prociso.com

TABLE OF CONTENTS

VULNERABILITIES OF THE MONTH

WHICH SHOULD BE REMEDIATED URGENTLY

Windows Scripting Languages Remote Code Execution Vulnerability (CVE-2022-41128)

“This vulnerability requires that a user with an affected version of Windows access a malicious server. An attacker would have to host a specially crafted server share or website. An attacker would have no way to force users to visit this specially crafted server share or website, but would have to convince them to visit the server share or website, typically by way of an enticement in an email or chat message.”.
Exploit is being sold on the market for USD $5k-$25k.
Reference: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41128

Microsoft released patches for Microsoft Exchange “ProxyNotShell” zero-days

Microsoft has released security updates for two actively exploited zero-day vulnerabilities tracked as CVE-2022-41040 and CVE-2022-41082. The attackers used zero-days to deploy Chinese Chopper web shells on compromised servers for persistence and data theft, as well as move laterally to other systems on the victims' networks.

Reference: https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-november-8-2022-kb5019758-2b3b039b-68b9-4f35-9064-6b286f495b1d

Image src: https://www.bleepingcomputer.com/

EMERGING THREATS

Hackers are spreading malware via trending TikTok challenge

Hackers are using a popular TikTok challenge to get people to download information-stealing malware. The campaign takes advantage of a TikTok trend called the “Invisible Challenge” in which people use a special video effect called “invisible body” to pose naked. The effect produces a blurred, contoured image of a person.

The hackers posted their own TikTok videos with links to fake software called “unfilter” that claims to be able to remove the TikTok filters and expose people’s naked bodies. The malware is hidden in malicious Python packages.

Reference:
https://therecord.media/hackers-are-spreading-malware-via-trending-tiktok-challenge-report/

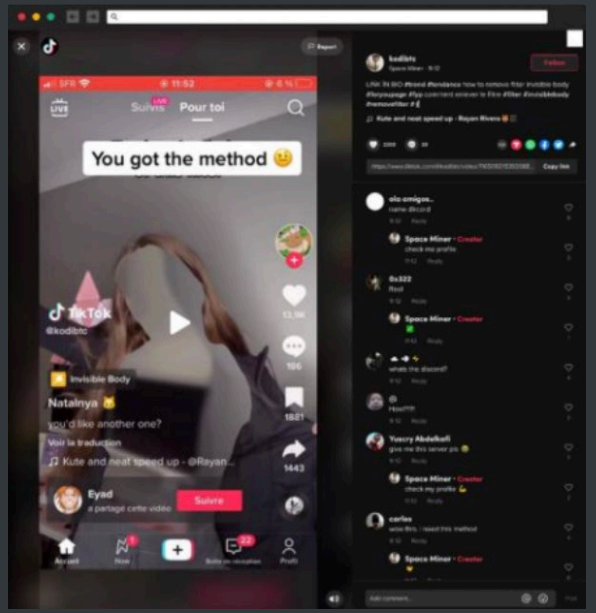


Image src: https://therecord.media

Pro CISO® can help you establish and manage Cyber Security resilience program to improve Cyber Security posture of your business.

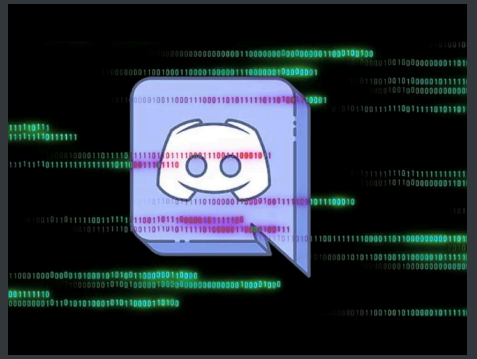
EMERGING THREATS

AXLocker ransomware steals Discord account and encrypts data

AxLocker ransomware targets consumers rather than the enterprise. If you become a victim of AxLocker, you should immediately change your Discord password, as it will invalidate the access token stolen by the ransomware.
As Discord has become the community of choice for NFT platforms and cryptocurrency groups, stealing a moderator token or other verified community member could allow threat actors to conduct scams and steal funds.

Reference:
https://blog.cyble.com/2022/11/18/axlocker-octocrypt-and-alice-leading-a-new-wave-of-ransomware-campaigns/

Pro CISO® can help you establish and manage Cyber Security resilience program to improve Cyber Security posture of your business.



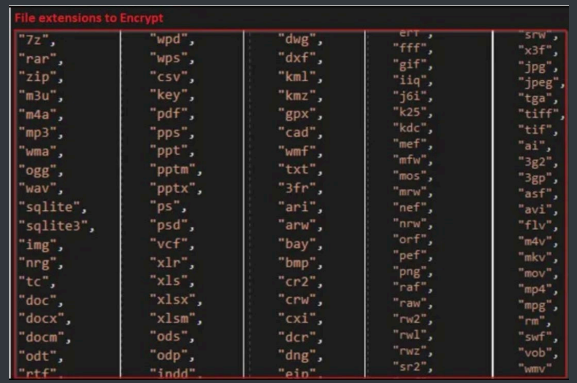


Image src: www.bleepingcomputer.com

RANSOMWARE TRENDS

New ways to deliver ransomware revealed by Microsoft

Threat actor tracked as DEV-0569 known to distribute various payloads, has led to the deployment of the Royal ransomware, which first emerged in September 2022 and is being distributed by multiple threat actors. Attacks have been observed targeting companies in The Netherlands and use new discovery techniques, defense evasion, and various post-compromise payloads, alongside increasing ransomware facilitation.

Reference: https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/ https://blog.thefir.io/dev-0569-threat-campaign-uncovered-2005c3294f81

Pro CISO® can help you establish and manage Ransomware resilience program to improve Cyber Security posture of your business.

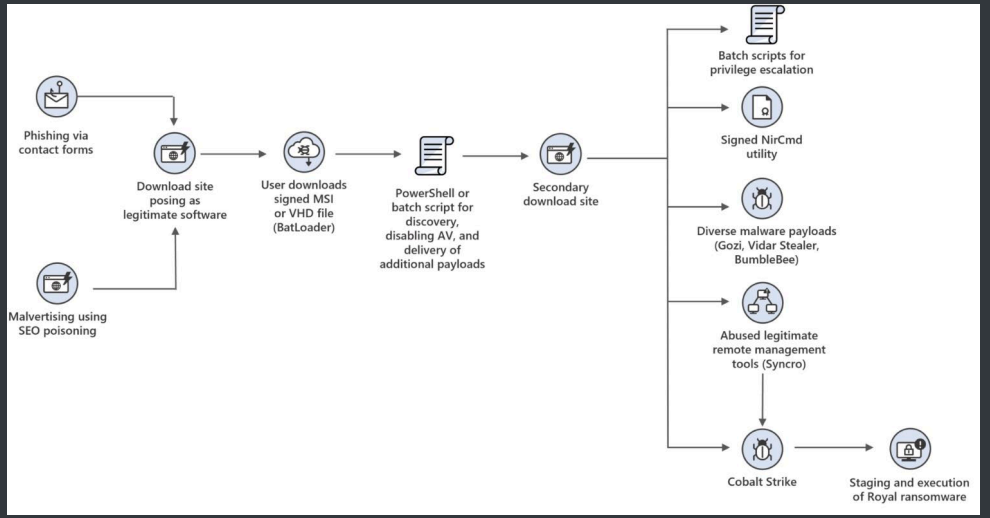


Image src: https://microsoft.com

CYBERSECURITY ADVISORIES

Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester

CISA and FBI are releasing this Cybersecurity Advisory (CSA) providing the suspected Iranian government-sponsored actors' tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help network defenders detect and protect against related compromises.
CISA and FBI encourage all organizations with affected VMware systems that did not immediately apply available patches or workarounds to assume compromise and initiate threat hunting activities. If suspected initial access or compromise is detected based on IOCs or TTPs described in this CSA, CISA and FBI encourage organizations to assume lateral movement by threat actors, investigate connected systems (including the DC), and audit privileged accounts. All organizations, regardless of identified evidence of compromise, should apply the recommendations in the Mitigations section of this CSA to protect against similar malicious cyber activity.
Reference: https://www.cisa.gov/uscert/ncas/alerts/aa22-320a

#StopRansomware: Hive Ransomware

FBI and CISA are releasing this joint CSA to disseminate known Hive IOCs and TTPs identified through FBI investigations as recently as November 2022.
FBI, CISA, and HHS encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.
Reference: https://www.cisa.gov/uscert/ncas/alerts/aa22-279a

PRO CISO® CYBER REVIEW

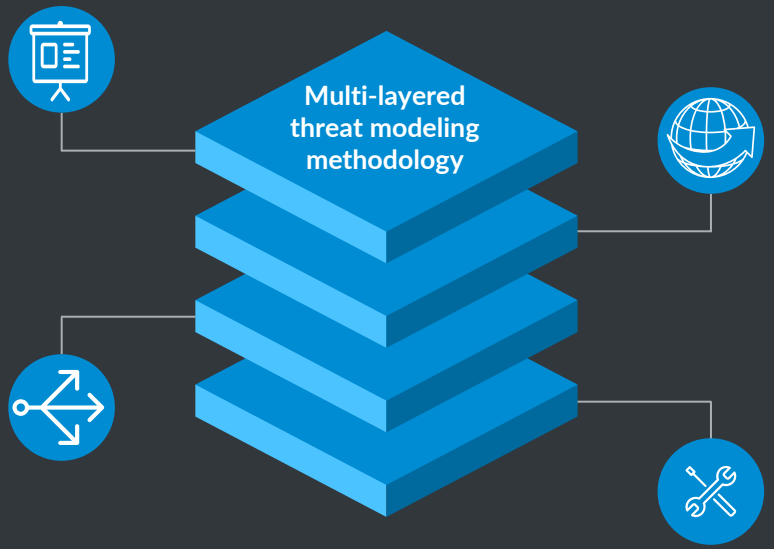
Detailed security review of the existing infrastructure to identify weaknesses and threat exposures

GENERAL ARCHITECTURE

Focus on the big picture, having visibility of the underlying layers, to gain visibility of the overall digital threat exposure of the business

NETWORK TOPOLOGY

Identify the network interconnection points, to verify the proper security of interfaces, the definition of internal segmentation and requirements for specific network security capabilities



APPLICATION SECURITY

Assess the application security and privacy posture, internal and 3rd party access, vulnerabilities, exposed APIs, implementation of proper Cloud security features, etc.

IT INFRASTRUCTURE

Analyze the IT infrastructure to identify security weaknesses, management of privileged and 3rd party and propose mitigating actions and operational optimizations

https://prociso.com AaaSK@prociso.com +31202117467

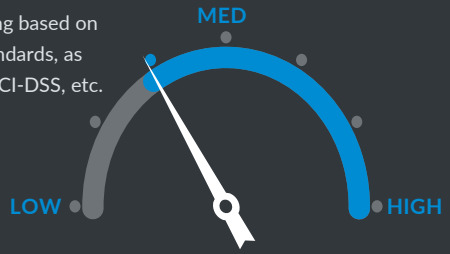
PRO CISO® MANAGED CYBER RISK

IDENTIFY COMPANY ASSETS

Integrate the company CMDB or create a central inventory of company assets, classified by importance to the business or data that is processed.

EASY INTEGRATION

Quick integration with the GRC in the Cloud, reporting based on international standards, as ISO27001, NIST, PCI-DSS, etc.



CYBER RISK STATUS

ASSESS GAPS TO STANDARDS

Verify the presence of appropriate security controls, that are required to mitigate the threats that the company is exposed to.

CONTINUOUSLY IMPROVE

Implement remediation plans that are prioritized on the higher risks. Repeat in periodical cycles and integrate with insight provided by Threat Intelligence and Vulnerability Management feeds.

Pro CISO® Managed GRC

Powered by OneTrust

https://prociso.com
AaaSK@prociso.com
+31202117467

PRO CISO® MANAGED THREAT INTELLIGENCE SERVICE

Pro CISO ®

THREAT ALERTING

Identification of potential attacks, data leakage, brand imitation and reputation, phishing attacks, external system vulnerability and VIP alerts to classify and respond to targeted threats.

OPERATIONAL AWARENESS

Reconnaissance and active monitoring of thousands of threat sources across the surface, deep and dark web produces real-time visibility into threats targeting your network, brand, assets, and people.

DARK WEB AND OSINT

Research the latest trends including malware, campaigns, TTPs, IOCs, and observables.

EXTERNAL EXPOSURES

Continuous monitoring and analysis of the company's domains, IP addresses, DLP indicators, mobile applications, social media pages, secret projects, technologies in use, VIP names and emails to identify and validate threats to the organization.

PRODUCT EXPLOITATION

Detection of product and supply chain exploitation techniques, PoCs and attacks.

Pro CISO® Managed TI

Powered by munitio SAGA®

AaaSK@prociso.com

PRO CISO® MANAGED VULNERABILITY MANAGEMENT

VULNERABILITY SCANNING

Frequent scans of infrastructure, applications and the Cloud for new vulnerabilities

PRIORITIZE PATCHING

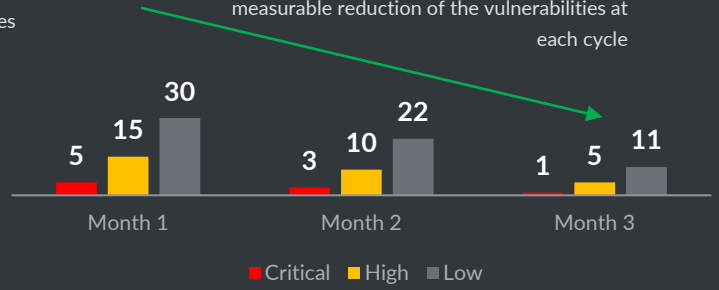
Personalized recommendations for implementing remediation actions based on severity, criticality, exposure, exploitability.

THREAT INTELLIGENCE

Proactive alerting of new exploits, zero-days, via the Pro CISO® Threat Intelligence Alerting service

VULNERABILITY EXPOSURE REDUCTION

Drives effective IT patching, provides measurable reduction of the vulnerabilities at each cycle



Pro CISO® Managed VM

Powered by Qualys.

PRO CISO® MANAGED SYSTEM ADMINISTRATORS

RAPID INTEGRATION

Leveraging the flexibility of the Cloud, you can rapidly and progressively integrate infrastructure and systems with the PAM solution

CONTROL ACCESS

Centrally manage administrator and 3rd party access only to the authorized resources

MONITOR ACTIVITY

Register all activities performed by administrators, for review preventively or in reaction to an incident

EMPOWER ADMINISTRATORS WITH FULL PRIVILEGES, WHILE REMAINING IN CONTROL OVER THEIR ACTIVITIES

PRO CISO® ENDPOINT ADMIN RIGHTS MANAGEMENT

Workstations with administrator privileges could be the entry point of a widespread corporate compromise, or cause software compliance issues

FROM FULL ADMIN RIGHTS

Employees are provided full administrator privileges on their laptops to be able to configure printers, Wi-Fi, install software, etc., however
providing end users with administrative privileges could cause massive risks, like an enterprise-wide cyber attack,
or
result in compliance issues for unlicensed software.

TO JUST ENOUGH PRIVILEGE

Employees have normal user privileges for everyday work activities, but
when necessary and with a justification, will be able to perform authorized administrative tasks,
and
install verified and approved software.

Pro CISO® Managed PAM

Powered by BeyondTrust

PRO CISO® CO-MANAGED SECURITY OPERATIONS

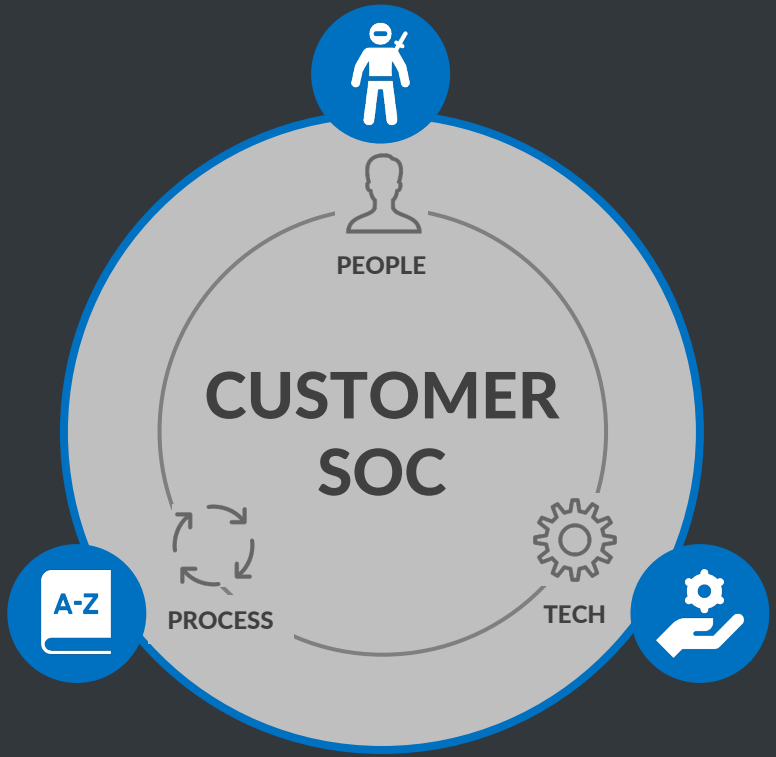
Pro CISO®

CO-MANAGED SOC

We help the Customer to implement a working Security Operations Center from scratch in just weeks, or support the further evolution of an existing SOC, to be ready to detect and respond to modern cyber attacks.

INCIDENT RESPONSE NINJAS

Experienced incident response ninjas, extending your SOC L1, L2 and L3 capacity with hands-on skills of responding to complex APT, ransomware attacks.



TAILOR MADE PROCESS LIBRARY

Tailor made SOC service catalogue, service description, processes and procedures, taking into account your organizational specifics, operational model based on real-world experience of building and running SOCs.

NEXT GEN SIEM EVOLUTION

Making your SIEM to make leap to next level , powered by modern technologies, automation, custom crafted use cases and detection techniques, enhancing visibility and security incident detection for on-prem, cloud and hybrid deployment scenarios.

https://prociso.com AaaSK@prociso.com +31202117467

CONTACT US

PRO CISO®

Cybersecurity insights

Threat Intelligence
powered by
SAGA®

munitio

AaaSK@prociso.com
https://prociso.com
LinkedIn

+31202117467