PRO CISO®

Cyber Security insights
September 2022

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

TABLE OF CONTENTS

1. Vulnerabilities of the Month
2. Emerging Threats
3. Ransomware Trends
4. Cybersecurity Advisories
5. Pro CISO® Introduction
6. Pro CISO® Managed Threat Intelligence Service
7. Pro CISO® Portfolio of Capabilities

VULNERABILITIES OF THE MONTH

WHICH SHOULD BE REMEDIATED URGENTLY

Remote Code Execution in Windows TCP/IP and Windows Internet Key Exchange (CVE-2022-34718, CVE-2022-34722)

Vulnerabilities're not actively exploited in a wild yet, but according to Microsoft exploitation is likely.
An unauthenticated attacker could send a specially crafted IP packet to a Windows node where IPSec is enabled, which could enable a remote code execution exploitation on that machine.

Microsoft patched vulnerability in Patch Tuesday.

Reference:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34718
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34722

Pro CISO recommends prioritizing those patches from Microsoft monthly update.

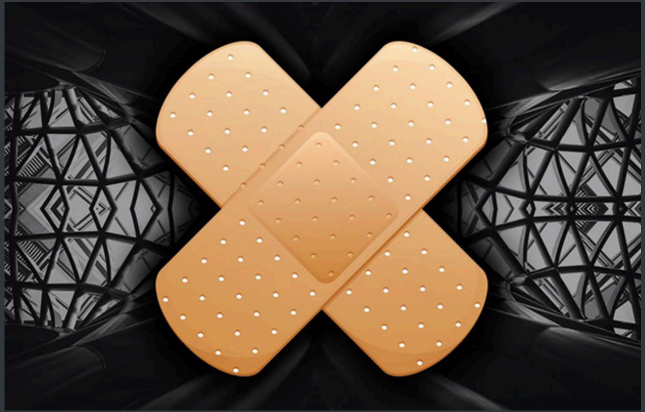


Image src: https://www.helpnetsecurity.com/

EMERGING THREATS

Threat actor hides a malicious payload in Windows Logo

The Witchetty espionage group using new malware in attacks on targets in the Middle East and Africa. Among the new tools being used by the group is a backdoor Trojan that employs steganography, a rarely seen technique where malicious code is hidden within an image. A DLL loader downloads a bitmap file from a GitHub repository. Disguising the payload in this fashion allowed the attackers to host it on a free, trusted service. Downloads from trusted hosts such as GitHub are far less likely to raise red flags than downloads from an attacker-controlled command-and-control (C&C) server.

Reference:
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage

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

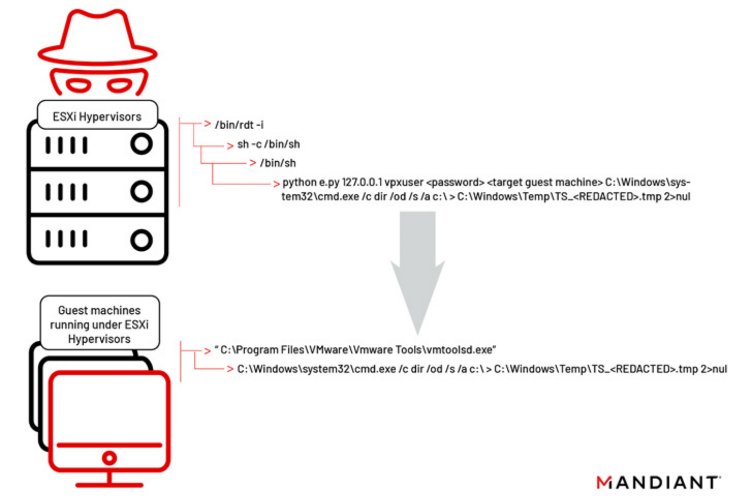
The image that the attackers used to hide the payload

EMERGING THREATS

New malware targets Vmware ESXi Hypervisors

Mandiant identified a novel malware ecosystem impacting VMware ESXi, Linux vCenter servers, and Windows virtual machines that enables a threat actor to execute commands on any guest VM in Hypervisor, transfer files and maintain persistent administrative access.

Reference:
https://core.vmware.com/vsphere-esxi-mandiant-malware-persistence
https://mandiant.com/resources/blog/esxi-hypervisors-malware-persistence
https://www.mandiant.com/resources/blog/esxi-hypervisors-detection-hardening



```
> /bin/rdt -i
    > sh -c /bin/sh
        > /bin/sh
            > python e.py 127.0.0.1 vpxuser <password> <target guest machine> C:\Windows\sys-
              tem32\cmd.exe /c dir /od /s /a c:\ > C:\Windows\Temp\TS_<REDACTED>.tmp 2>nul

> " C:\Program Files\VMware\Vmware Tools\vmtoolsd.exe"
    > C:\Windows\system32\cmd.exe /c dir /od /s /a c:\ > C:\Windows\Temp\TS_<REDACTED>.tmp 2>nul
```

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

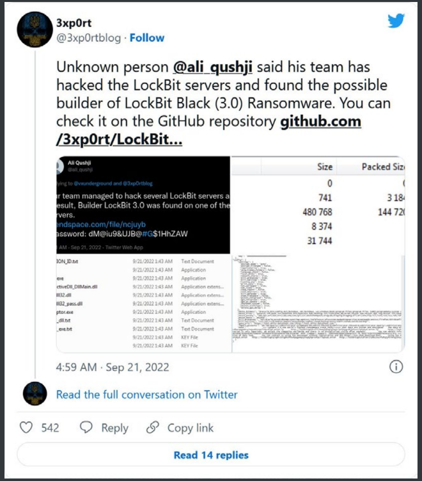
RANSOMWARE TRENDS

Leaked Lockbit 3.0 builder used by different ransomware gangs in attacks

Lockbit has recently suffered a breach in which angry developer leaked a source code of ransomware builder allowing anyone to build encryptor/decryptor for attacks.
Builder was used by The Bloody ransomware gang in attacks against organizations in Ukraine and USA.
As the leaked LockBit 3.0 ransomware builder is easily customizable by other threat actors, we will see other threat actors soon using it in their own attacks.

Reference: https://www.bleepingcomputer.com/news/security/leaked-lockbit-30-builder-used-by-bl00dy-ransomware-gang-in-attacks/

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



3xp0rt
@3xp0rtblog · Follow

Unknown person @ali_qushji said his team has hacked the LockBit servers and found the possible builder of LockBit Black (3.0) Ransomware. You can check it on the GitHub repository github.com/3xp0rt/LockBit...

Ali Qushji
@ali_qushji
ying to @vxunderground and @3xp0rtblog
r team managed to hack several LockBit servers a
esult, Builder LockBit 3.0 was found on one of the
rvers.
endspace.com/file/ncjuyb
assword: dM@iu9&UJB@#G$1HhZAW
AM · Sep 21, 2022 · Twitter Web App

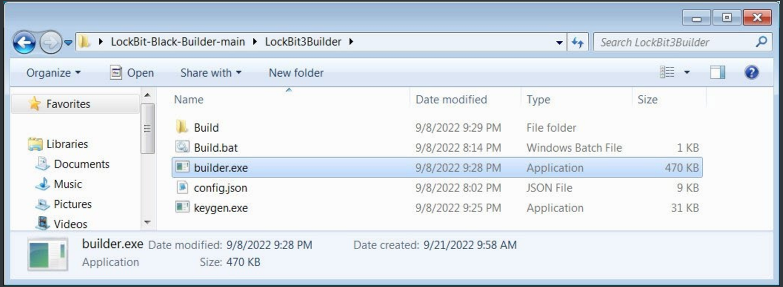
Size	Packed Siz
0	(
741	3 18
480 768	144 72
8 374	
31 744	

```
ION_ID.txt            9/21/2022 1:43 AM   Text Document
                      9/21/2022 1:43 AM   Application
exe                   9/21/2022 1:43 AM   Application
ctiveDll_DllMain.dll  9/21/2022 1:43 AM   Application extens...
ll32.dll              9/21/2022 1:43 AM   Application extens...
ll32_pass.dll         9/21/2022 1:43 AM   Application extens...
ptor.exe              9/21/2022 1:43 AM   Application
_dll.txt              9/21/2022 1:43 AM   Text Document
_exe.txt              9/21/2022 1:43 AM   Text Document
                      9/21/2022 1:43 AM   KEY File
                      9/21/2022 1:43 AM   KEY File
```

4:59 AM · Sep 21, 2022

Read the full conversation on Twitter

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



Name	Date modified	Type	Size
Build	9/8/2022 9:29 PM	File folder	
Build.bat	9/8/2022 8:14 PM	Windows Batch File	1 KB
builder.exe	9/8/2022 9:28 PM	Application	470 KB
config.json	9/8/2022 8:02 PM	JSON File	9 KB
keygen.exe	9/8/2022 9:25 PM	Application	31 KB

builder.exe Date modified: 9/8/2022 9:28 PM Date created: 9/21/2022 9:58 AM
Application Size: 470 KB

CYBERSECURITY ADVISORIES

Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations

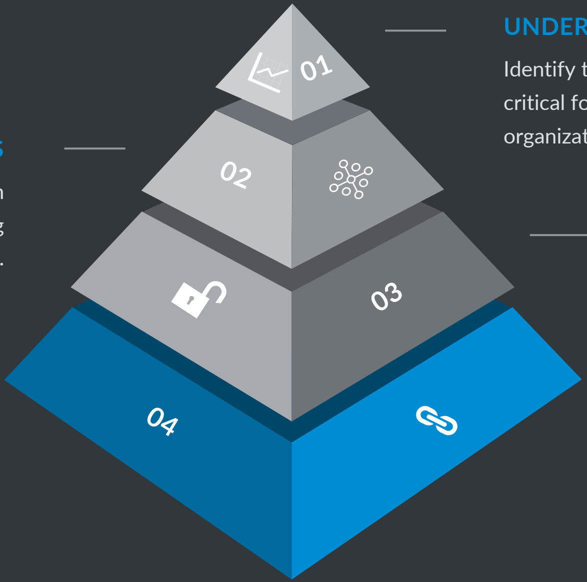
Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities, the authoring agencies have observed Iranian government-sponsored APT actors scanning for and/or exploiting the known Fortinet FortiOS and Microsoft Exchange server vulnerabilities since early 2021 to gain initial access to a broad range of targeted entities.
Reference: https://www.cisa.gov/uscert/ncas/alerts/aa22-257a

Iranian State Actors Conduct Cyber Operations Against the Government of Albania

In July 2022, Iranian state cyber actors—identifying as "HomeLand Justice"—launched a destructive cyber attack against the Government of Albania which rendered websites and services unavailable. A FBI investigation indicates Iranian state cyber actors acquired initial access to the victim's network approximately 14 months before launching the destructive cyber attack, which included a ransomware-style file encryptor and disk wiping malware. The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating e-mail content.
Reference: https://www.cisa.gov/uscert/ncas/alerts/aa22-264a

PRO CISO® INTRODUCTION

Business driven methodology to support the implementation of a sustainable, custom-fit and prioritized cybersecurity strategy.



UNDERSTAND THE BUSINESS

Identify the business processes that are critical for the success of the organization.

IDENTIFY ASSETS

Map systems, classify the information processed and the stakeholders owning or processing it.

ASSESS RISKS

Baseline against NIST, ISO 27001, PCI, etc. frameworks, using smart GRC/IRM platforms. Identify Threats and Vulnerabilities.

BUILD RESILIENCE

Prioritized deployment of security capabilities to protect, detect, respond and rapidly recover from adverse events. All while minimizing disruption.

PRO CISO® MANAGED THREAT INTELLIGENCE SERVICE

THREAT ALERTING

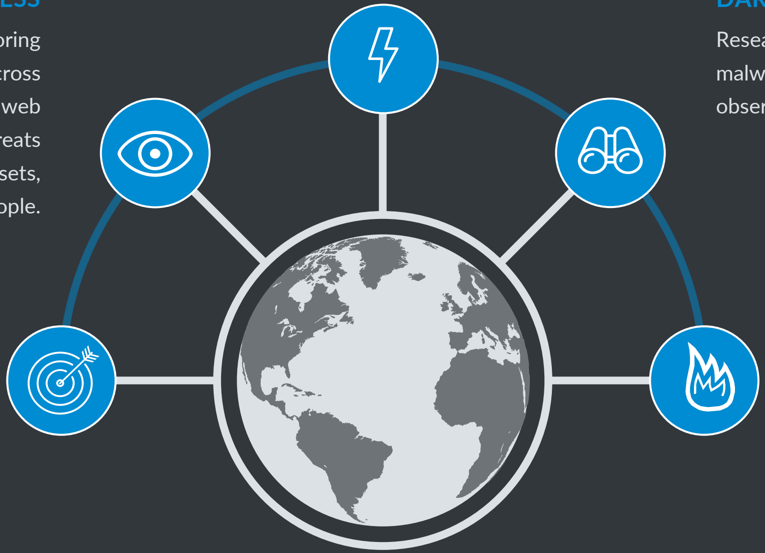
Identification of potential attacks, data leakage, brand imitation and reputation, phishing attacks, external system vulnerability and VIP alerts to classify and respond to targeted threats.

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

PRO CISO® MANAGED CYBER RISK

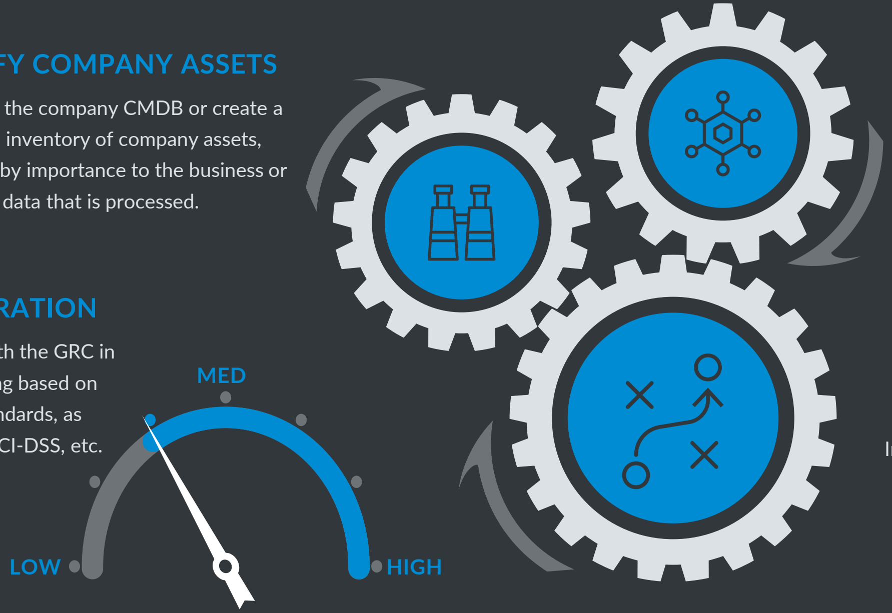
Pro CISO®

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

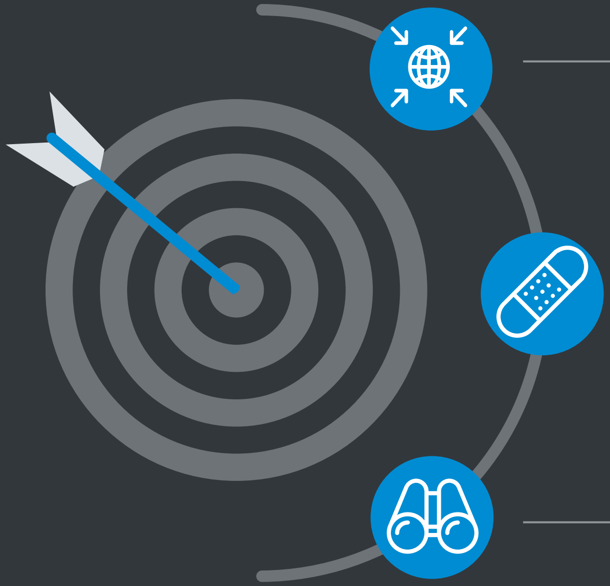
Verify the presence of appropriate security controls, that are required to mitigate the threats that the company is exposed to.

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

PRO CISO® MANAGED VULNERABILITY MANAGEMENT



VULNERABILITY SCANNING

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

PRIORITIZE PATCHING

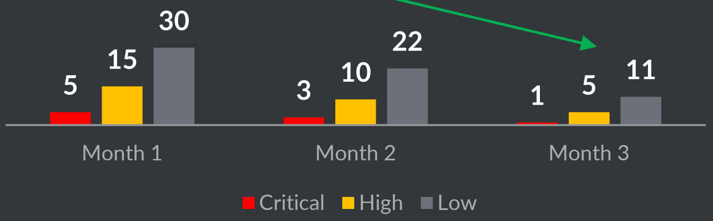
Personalized recommendations for implementing remediation actions based on risk mitigation

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

PRO CISO® MANAGED PRIVILEGED ACCESS

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

Pro CISO® Managed PAM

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

CONTACT US

PRO CISO®

Cybersecurity insights

Threat Intelligence
powered by
SAGA®

munitio

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

+31202117467

☎ B 💬