SEC Consult

an Eviden business

Resilience Rising

Countering the Threat Actors Behind Black Basta Ransomware

Angelo Violetti
Security Consultant
1.0 | 24/10/2023

SEC Consult

an Eviden business

Angelo Violetti

Digital Forensics & Incident Response (DFIR) Consultant

SEC Consult (Schweiz) AG

- Joined SEC Consult in 2022 after 2 years in a big 4
- 3.5 years of experience in DFIR
- Analyst for The DFIR Report
- Master's Degree in Cyber Security at Politecnico di Milano
- SANS GCFA, CRTO, eCMAP, Xintra Cloud Security, Sektor7 Malware Dev., AZ900

SEC Consult

an Eviden business

Index

Ransomware ecosystem

RaaS business model and human-operated ransomware

Description

Nowadays, **ransomware attacks** are **directly driven** by **individual criminals** (i.e., affiliates) who are **part** of **wider groups** that are structured as real organizations with specific roles for every member. Therefore, **behind ransomware intrusions**, there are **humans** who have different skills, objectives and behaviours.

Ransomware as a service actors

Initial access brokers

- Mainly **sell** company **credentials** or **access** to **infrastructures** infected via malware

Ransomware operators

- **Develop** the **ransomware** builder
- **Manage** the **infrastructure** which hosts the data leak site
- **Recruit** affiliates
- **Obtain** a **percentage** of the payments made by the victims

Ransomware affiliates

- **Join** a ransomware **group**
- **Perform post-exploitation** activities
- **Exfiltrate** and **encrypt** victims' data
- **Communicate** with the **victims** to obtain the payments

Money launderers

- **Launder** the **money** made by ransomware operators and affiliates

Human-operated ransomware

Ransomware characteristics and how to protect from them

Ransomware attack characteristics

1. The **main objective** of ransomware **operators** and **affiliates** is to obtain **financial gain**, which depends on the **number** of **victims** and their **size**.

2. It's **crucial** to **encrypt business-critical data** to force the victim to pay the ransom.

Ransomware group specific

3. To perform a **successful attack**, affiliates follow specific **playbooks** which detail the intrusion procedures. Moreover, the **reliability** and **defense evasion capabilities** of the **tools** used are crucial.

4. To perform an **attack efficiently** (to move to the next victim), affiliates try to **exploit common misconfigurations** or **vulnerabilities** in organizations' environments (e.g., Kerberoasting to domain admin).

Recommendations

1. **Paying** the **ransom** means **funding** further **criminal actions** and **making** this type of **activity profitable**.

2. **Identify** where the **company's data resides** and **protect it** according to its importance.

3. Having **knowledge** of the **tactics**, **techniques**, **procedures**, and **tools** used by ransomware groups during their attacks.

4. **Minimize** the **number** of **misconfigurations** or **vulnerabilities easily exploitable** to slow down the attack and make it inefficient.

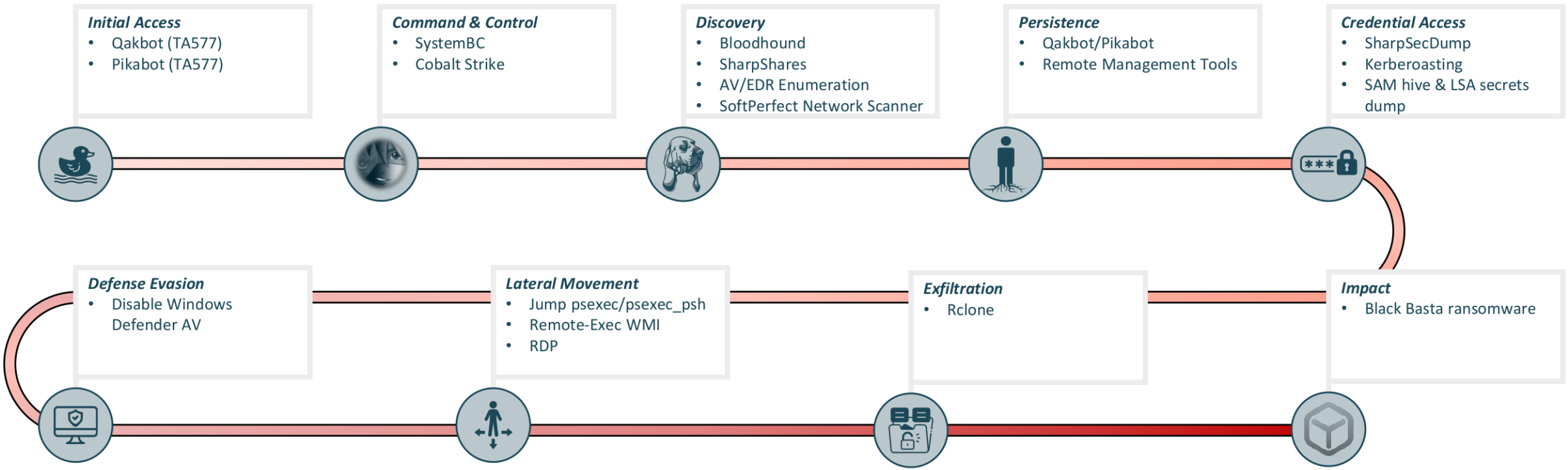
Black Basta

TTPs and tools used

Description

Black Basta is a **ransomware-as-a-service** (RaaS) that was discovered in **April 2022** and quickly gained notoriety due to the high number of victims hit by the criminal group, according to BlackBerry, more than 100 in just the first months.

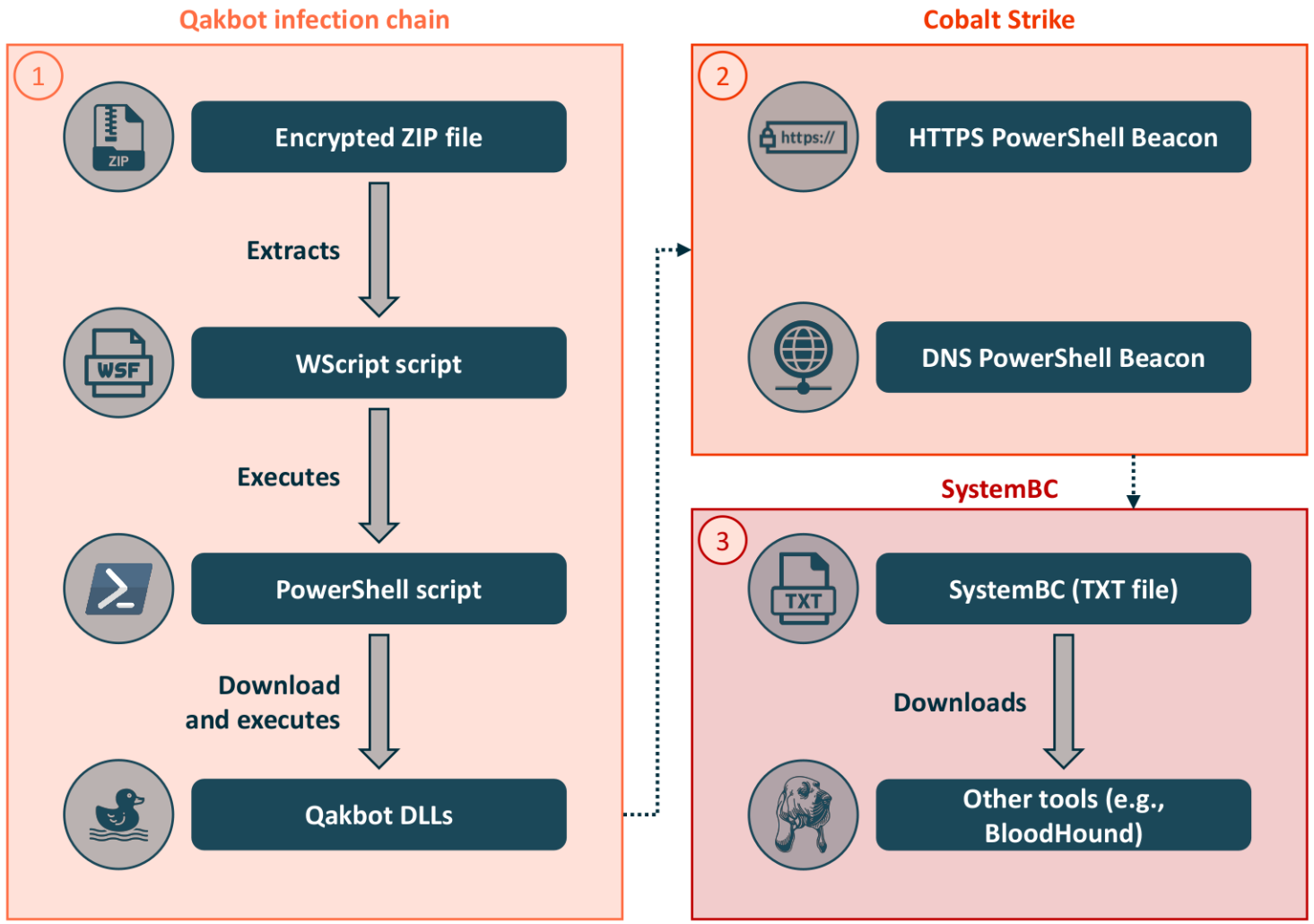
Attack chain



Source: https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/black-basta

Countering Black Basta

Initial access and command and control



Prevent, Detect & Remediate

Prevention

- Perform periodic awareness activities
- Restrict the usage of PowerShell to only specific groups of users through AppLocker
- Enable PowerShell Constrained Language Mode
- Enable Attack Surface Reduction Rules (e.g. block the execution of potentially obfuscated scripts)
- Block Windows executables making connections when they should not (e.g., WScript.exe) through Windows Firewall

Monitoring

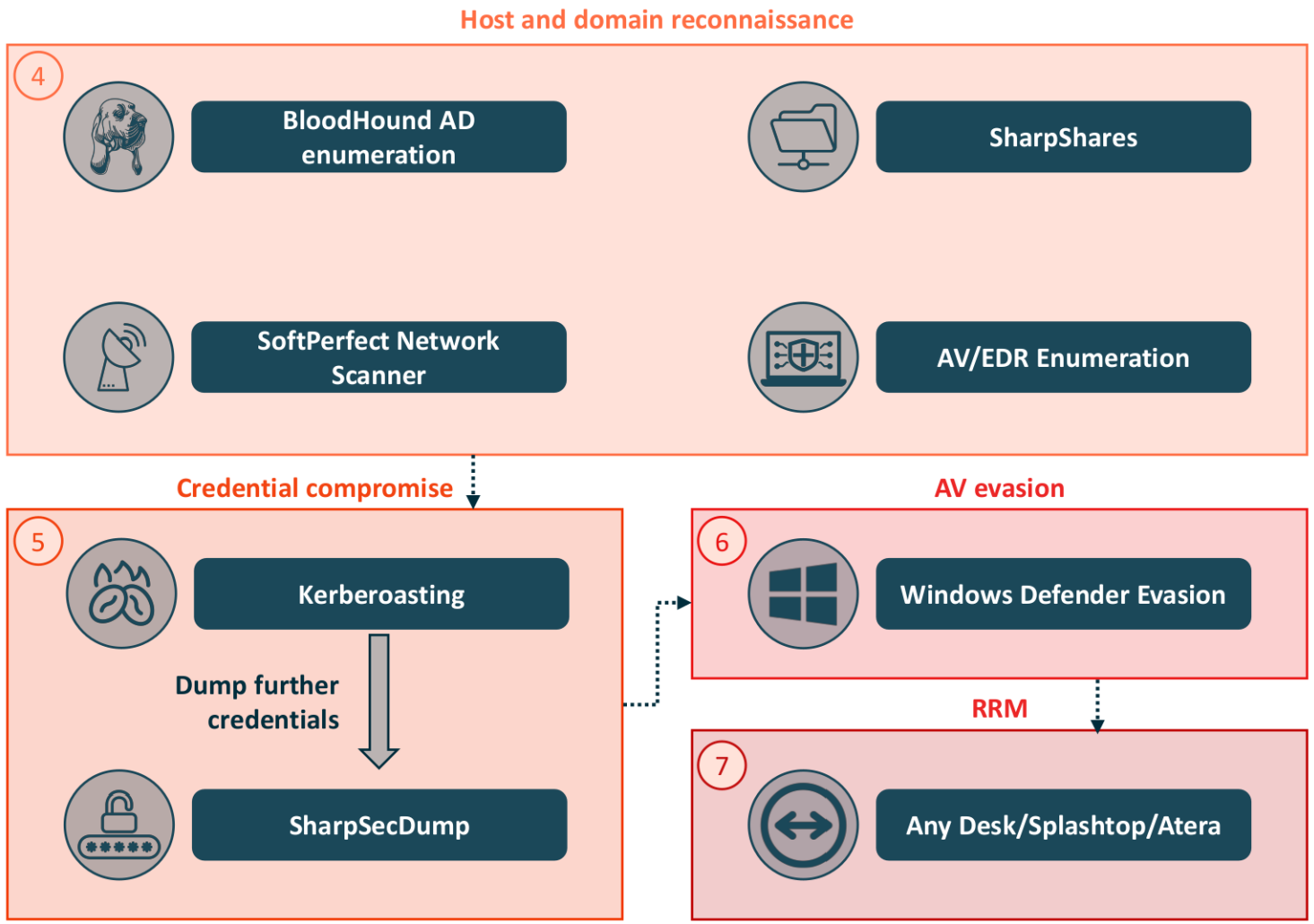
- Monitor DNS queries potentially related to Cobalt Strike through the following regex:

[a-z0-9]{8}+.[a-z0-9]+.[a-z0-9]+.[A-Za-z]{2,6}$

- Define detection rules for Cobalt Strike behaviours (e.g., rundll32.exe without a command line)
- Hunt for masqueraded executable files (e.g., .TXT)

Countering Black Basta

Discovery, credential dumping, defense evasion and persistence



Prevent, Detect & Remediate

Prevention

- Strong password for service accounts
- Apply the least privilege principle for service accounts

Monitoring

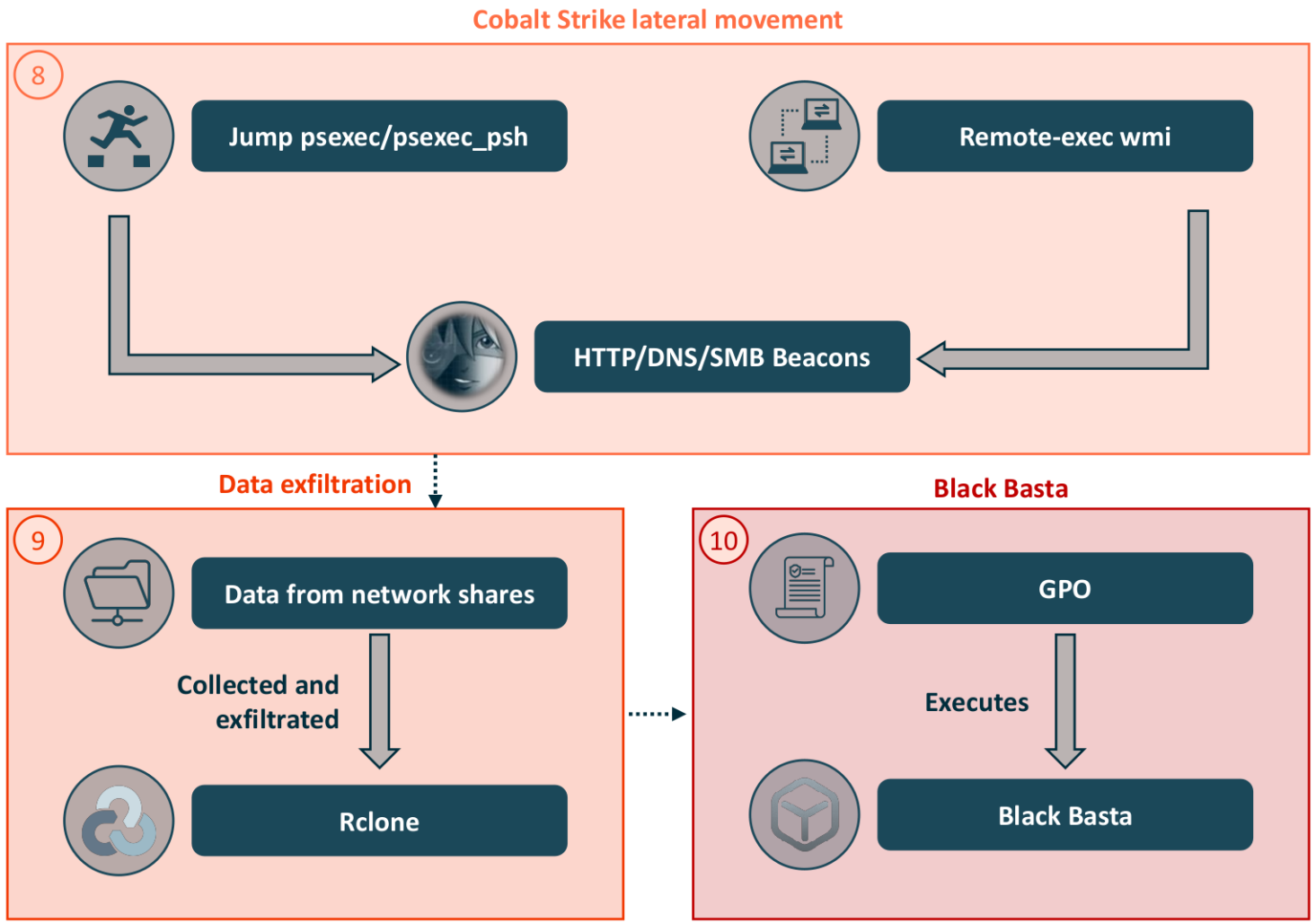
- Define detection rules for the most common enumeration commands (e.g., whoami /priv, net users, etc.)
- Define detection rules for commands used to disable Windows Defender
- Define detection rules for commonly used RMM tools

Deception

- Create fake Kerberoastable / ASREPRoastable users
- Create accounts with fake passwords in the user's description
- Create decoy files in shared folders containing fake user credentials

Countering Black Basta

Lateral movement, exfiltration and impact



Prevent, Detect & Remediate

Prevention

- Adopt and periodically review backup plans
- Adopt a crisis management procedure
- Ensure that the virtualized environments are sufficiently protected
- Encrypt business-critical data

Monitoring

- Define detection rules for detecting PsExec and WMI Cobalt Strike lateral movements
- Define detection rules for identifying Rclone usage
- Monitor for incoming logins coming from systems having a hostname like WIN-*

Remediation

- Determine the scope of the incident and isolate the impacted systems
- Start performing an incident response activity

Further recommendations

Countering ransomware strategy

Indicent Response Maturity Assessment

Assess the organization's **maturity** related to the **identification** and **response** to cyber **security incidents**. IRMA identifies the **gaps** between an organization's **target** state and the **as-is state**, providing recommendations to **improve cyber resilience**.

Perform periodic assessments of the external and internal infrastructure to promptly **detect** and **remediate vulnerabilities** and **misconfigurations** that could be exploited by threat actors.

Penetration Testing

Detect & Respond

Protect the organization's **assets** through **endpoint detection** and **response technologies** and **services** which integrate static and behavioural analysis to block malicious actions.

Evaluate an organization's **incident response capabilities** by either testing a specific playbook in a close to a real-life scenario or testing the internal processes and communication during a simulated incident.

War Games

Purple Teaming

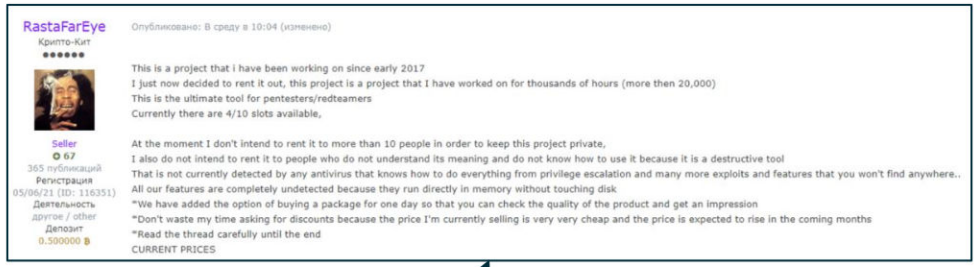
Assess the organization's capabilities to **detect ransomware TTPs** and **tools** and improve them by identifying gaps and improvement actions.

Adopt a 24/7 **rapid response team** to handle a cyber-attack within an SLA-specific timeframe to **quickly remediate** and **reduce** the **potential impacts**.

IR Retainer

Black Basta & TA577

Last months key events



RastaFarEye announced a new malware called DarkGate Loader on xss.is and exploit.in

June 16, 2023

August 22, 2023

Black Basta published the last August's victim on their website

FBI disrupted the Qakbot infrastructure used also to deliver the malware by TA577

August 25, 2023

September 22, 2023

TA577 has started spreading DarkGate malware

Black Basta came back publishing new victims on their website

October 11, 2023

TA557 has started using the previous Qakbot infrastructure (AA and BB) for delivering **DarkGate, Pikabot and IcedID**

Sources:

- https://www.zerofox.com/blog/the-underground-economist-volume-3-issue-12/
- https://twitter.com/malware_traffic/status/1709954582539882593
- https://twitter.com/pr0xylife/status/1705331101365891455

Legend

TA577 event-related

Black Basta event-related

Questions?

Thank you!

Dou you have any further questions?
For more information please contact:

Angelo Violetti
Digital Forensics & Incident Response Consultant
angelo.violetti@sec-consult.com
+41791274527