Detecting the Unknown: Revealing Uncategorized Ransomware Using Darktrace

de.darktrace.com/blog/detecting-the-unknown-revealing-uncategorised-ransomware-using-darktrace

25

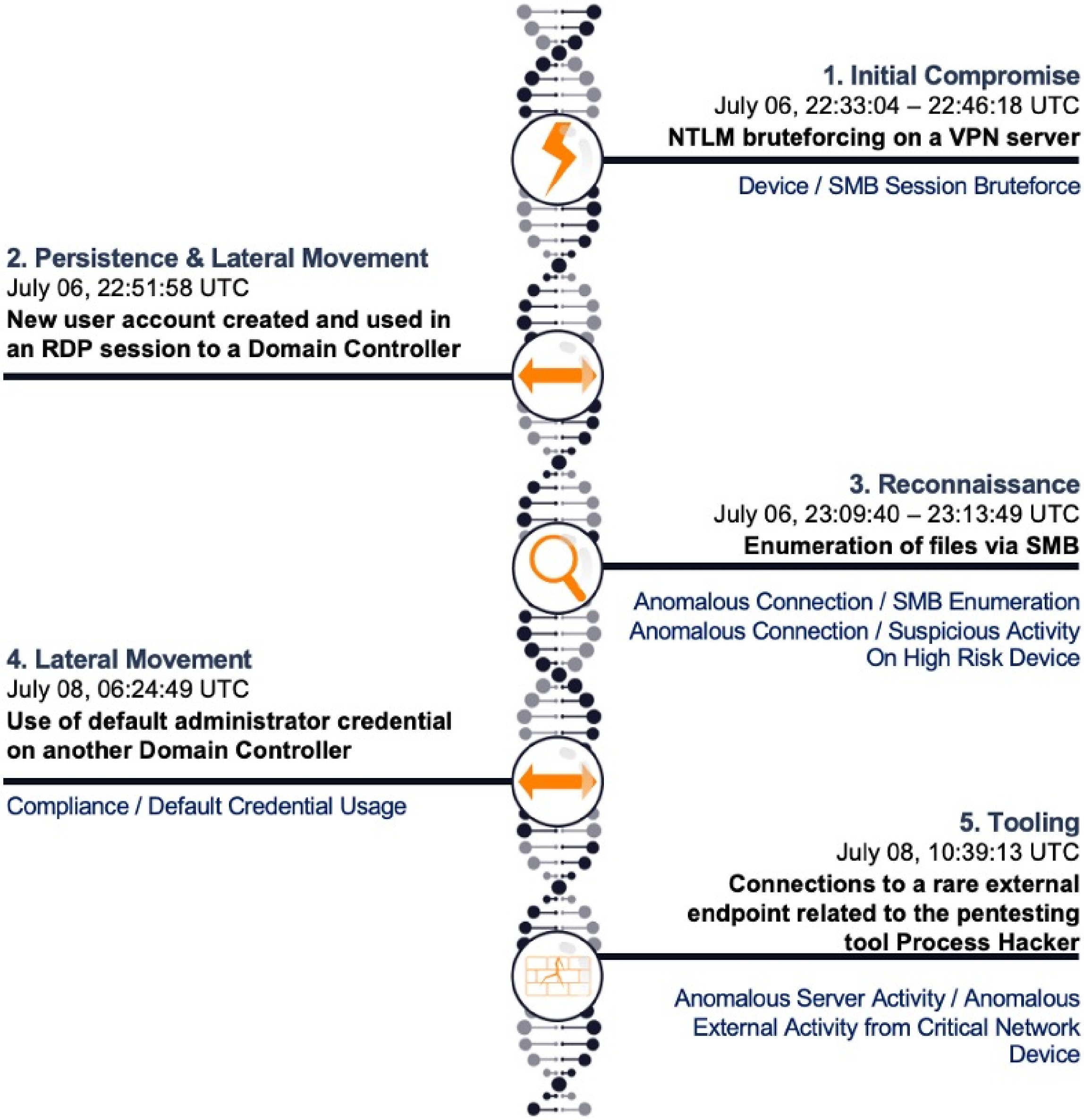
Aug 2022

25

Aug 2022

Uncategorized attacks happen frequently, with new threat groups and malware continually coming to light. Novel and known threat groups alike are changing their C2 domains, file hashes and other threat infrastructure, allowing them to avoid detection through traditional signature and rule-based techniques. Zero-day exploitation has also become increasingly apparent – a recent Mandiant report revealed that the number of identified zero-days in 2021 had dramatically increased from 2020 (80 vs 32). More specifically, the number of zero-days exploited by ransomware groups was, and continues to be, on an upward trend [1]. This trend appears to have continued into 2022. Given the unknown nature of these attacks, it is challenging to defend against them using traditional signature and rule-based approaches. Only those anomaly-based solutions functioning via deviations from normal behavior in a network, will effectively detect these threats.

It is particularly important that businesses can quickly identify threats like ransomware before the end-goal of encryption is reached. As the variety of ransomware strains increases, so do the number which are uncategorized. Whilst zero-days have recently been explored in another Darktrace blog, this blog looks at an example of a sophisticated novel ransomware attack that took place during Summer 2021 which Darktrace DETECT/Network detected ahead of it being categorized or found on popular OSINT. This occurred within the network of an East African financial organization.



1. Initial Compromise
July 06, 22:33:04 – 22:46:18 UTC
NTLM bruteforcing on a VPN server
Device / SMB Session Bruteforce

2. Persistence & Lateral Movement
July 06, 22:51:58 UTC
New user account created and used in an RDP session to a Domain Controller

3. Reconnaissance
July 06, 23:09:40 – 23:13:49 UTC
Enumeration of files via SMB
Anomalous Connection / SMB Enumeration
Anomalous Connection / Suspicious Activity On High Risk Device

4. Lateral Movement
July 08, 06:24:49 UTC
Use of default administrator credential on another Domain Controller
Compliance / Default Credential Usage

5. Tooling
July 08, 10:39:13 UTC
Connections to a rare external endpoint related to the pentesting tool Process Hacker
Anomalous Server Activity / Anomalous External Activity from Critical Network Device

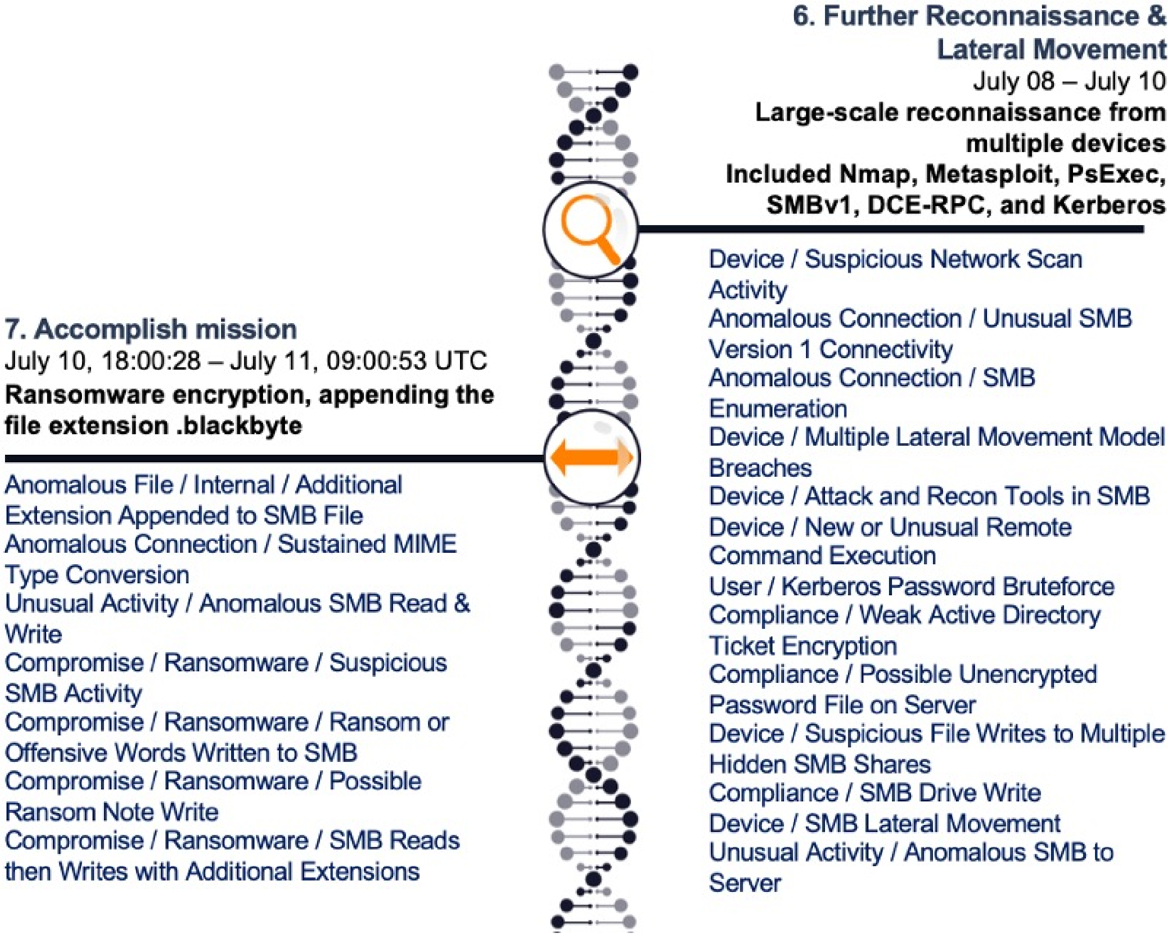
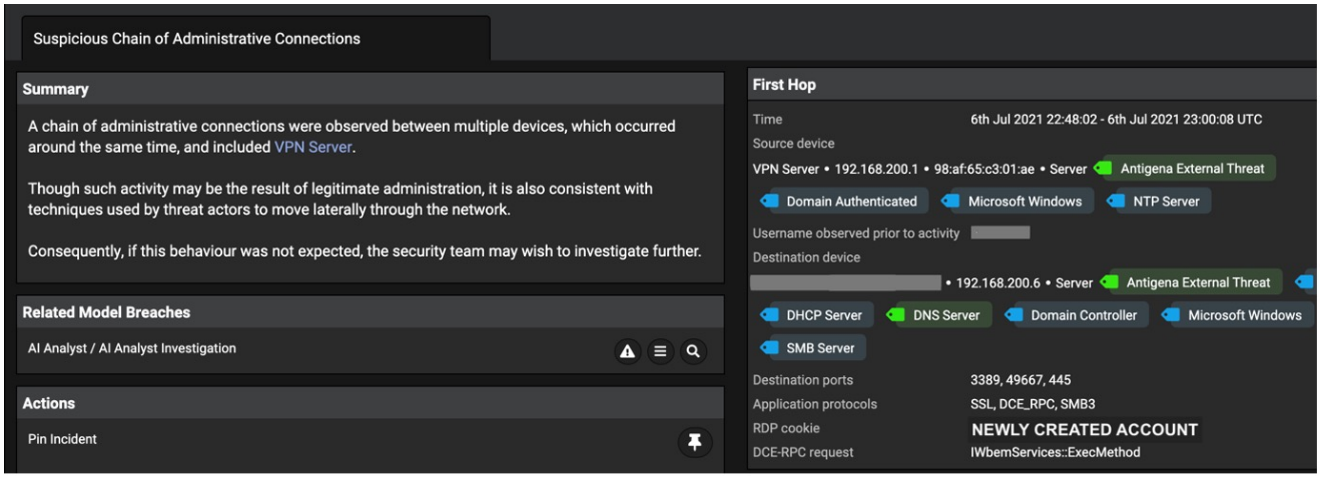

6. Further Reconnaissance & Lateral Movement
July 08 – July 10
Large-scale reconnaissance from multiple devices
Included Nmap, Metasploit, PsExec, SMBv1, DCE-RPC, and Kerberos
Device / Suspicious Network Scan Activity
Anomalous Connection / Unusual SMB Version 1 Connectivity
Anomalous Connection / SMB Enumeration
Device / Multiple Lateral Movement Model Breaches
Device / Attack and Recon Tools in SMB
Device / New or Unusual Remote Command Execution
User / Kerberos Password Bruteforce
Compliance / Weak Active Directory Ticket Encryption
Compliance / Possible Unencrypted Password File on Server
Device / Suspicious File Writes to Multiple Hidden SMB Shares
Compliance / SMB Drive Write
Device / SMB Lateral Movement
Unusual Activity / Anomalous SMB to Server
7. Accomplish mission
July 10, 18:00:28 – July 11, 09:00:53 UTC
Ransomware encryption, appending the file extension .blackbyte
Anomalous File / Internal / Additional Extension Appended to SMB File
Anomalous Connection / Sustained MIME Type Conversion
Unusual Activity / Anomalous SMB Read & Write
Compromise / Ransomware / Suspicious SMB Activity
Compromise / Ransomware / Ransom or Offensive Words Written to SMB
Compromise / Ransomware / Possible Ransom Note Write
Compromise / Ransomware / SMB Reads then Writes with Additional Extensions

Figure 1- Timeline of (then-uncategorized) Blackbyte ransom attack

On the 6th of July 2021, multiple user accounts were brute-forced on an external-facing VPN server via NTLM. Notably this included attempted logins with the generic account ‘Administrator’. Darktrace alerted to this initial bruteforcing activity, however as similar attempts had been made against the server before, it was not treated as a high-priority threat.

Following successful bruteforcing on the VPN, the malicious actor created a new user account which was then added to an administrative group on an Active Directory server. This new user account was subsequently used in an RDP session to an internal Domain Controller. Cyber AI Analyst picked up on the unusual nature of these administrative connections in comparison to normal activity for these devices and alerted on it (Figure 2).



Suspicious Chain of Administrative Connections

Summary

A chain of administrative connections were observed between multiple devices, which occurred around the same time, and included VPN Server.

Though such activity may be the result of legitimate administration, it is also consistent with techniques used by threat actors to move laterally through the network.

Consequently, if this behaviour was not expected, the security team may wish to investigate further.

Related Model Breaches

AI Analyst / AI Analyst Investigation

Actions

Pin Incident

First Hop

Time: 6th Jul 2021 22:48:02 - 6th Jul 2021 23:00:08 UTC

Source device

VPN Server • 192.168.200.1 • 98:af:65:c3:01:ae • Server · Antigena External Threat · Domain Authenticated · Microsoft Windows · NTP Server

Username observed prior to activity: [redacted]

Destination device

[redacted] • 192.168.200.6 • Server · Antigena External Threat · DHCP Server · DNS Server · Domain Controller · Microsoft Windows · SMB Server

Destination ports: 3389, 49667, 445

Application protocols: SSL, DCE_RPC, SMB3

RDP cookie: NEWLY CREATED ACCOUNT

DCE-RPC request: IWbemServices::ExecMethod

Figure 2: AI Analyst detected the suspicious nature of the initial lateral movement. RDP, DCE-RPC, and SMB connections were seen from the VPN server to the domain controller using the newly created account. Note: this screenshot is from DETECT/Network v.5

Less than 20 minutes later, significant reconnaissance began on the domain controller with the new credential. This involved SMB enumeration with various file shares accessed including sensitive files such as the Security Account Manager (samr). This was followed by a two-day period of downtime where the threat actor laid low.

On the 8th of July, suspicious network behavior resumed – the default Administrator credential seen previously was also used on a second internal domain controller. Connections to a rare external IP were made by this device a few hours later. OSINT at the time suggested these connections may have been related to the use of penetration testing tools, in particular the tool Process Hacker [2].

Over the next two days reconnaissance and lateral movement activities occurred on a wider scale, originating from multiple network devices. A wide variety of techniques were used during this period:

- Exploitation of legitimate administrative services such as PsExec for remote command execution.
- Taking advantage of legacy protocols still in use on the network like SMB version 1.
- Bruteforcing login attempts via Kerberos.
- The use of other penetration testing tools including Metasploit and Nmap. These were intended to probe for vulnerabilities.

On the 10th of July, ransomware was deployed. File encryption occurred, with the extension '.blackbyte' being appended to multiple files. At the time there were no OSINT references to this file extension or ransomware type, therefore any signature-based solution would have struggled to detect it. It is now apparent that BlackByte ransomware had only appeared a few weeks earlier and, since then, the Ransomware-as-a-Service group has been attacking businesses and critical infrastructure worldwide [3]. A year later they still pose an active threat.

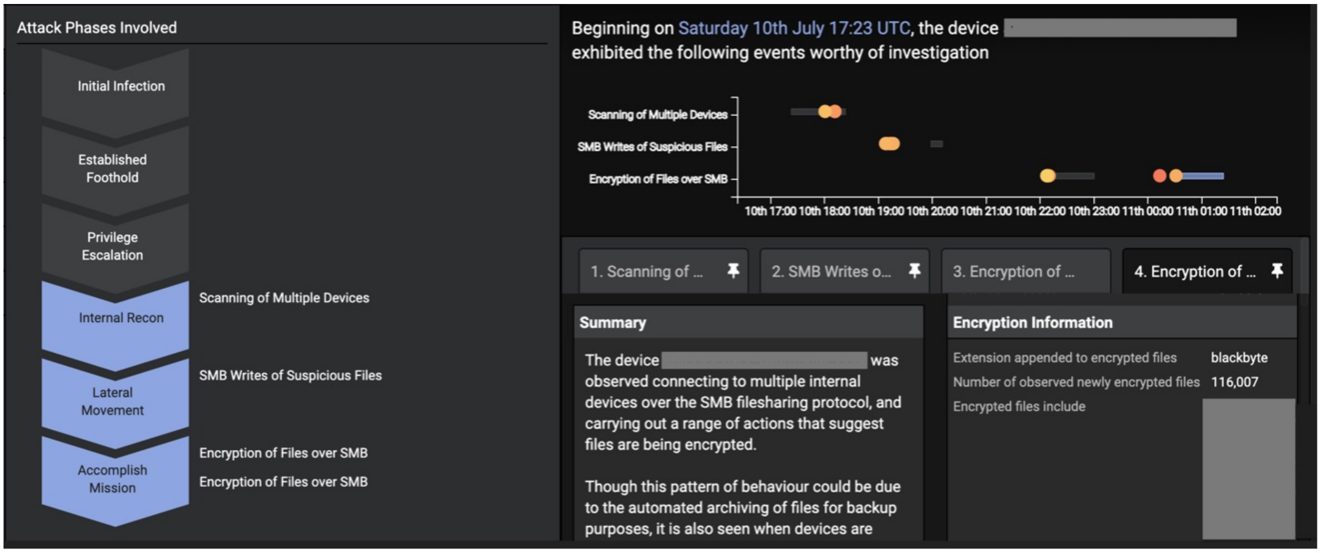
The use of living-off-the-land techniques, popular penetration testing tools, and a novel strain of ransomware meant the attackers were able to move through the environment without giving away their presence through known malware-signatures. Although a traditional security solution would identify some of these actions, it would struggle to link these separate activities. The lack of attribution, however, had no bearing on Darktrace's ability to detect the unusual behavior with its anomaly-based methods.

While this customer had RESPOND enabled at the time of this attack, its manual configuration meant that it was unable to act on the devices engaging in encryption. Nevertheless, a wide range of high-scoring Darktrace DETECT/Network models breached which were easily visible within the customer's threat tray. This included multiple Enhanced Monitoring models that would have led to Proactive Threat Notifications (PTN) being alerted had the customer subscribed to the service. Whilst the attack was not prevented in this case, Darktrace analysts were able to give support to the customer via Ask the Expert (ATE), providing in-depth analysis of the compromise including a list of likely compromised devices and credentials. This helped the customer to work on post-compromise recovery effectively and ensured the ransomware had reduced impact within their environment.

Schlussfolgerung

While traditional security solutions may be able to deal well with ransomware that uses known signatures, AI is needed to spot new or unknown types of attack – a reliance on signatures will lead to these types of attack being missed.

Remediation can also be far more difficult if a victim doesn't know how to identify the compromised devices or credentials because there are no known IOCs. Darktrace model breaches will highlight suspicious activity in each part of the cyber kill chain, whether involving a known IOC or not, helping the customer to efficiently identify areas of compromise and effectively remediate (Figure 3).



Beginning on Saturday 10th July 17:23 UTC, the device [redacted] exhibited the following events worthy of investigation

Summary

The device [redacted] was observed connecting to multiple internal devices over the SMB filesharing protocol, and carrying out a range of actions that suggest files are being encrypted.

Though this pattern of behaviour could be due to the automated archiving of files for backup purposes, it is also seen when devices are

Encryption Information

Extension appended to encrypted files	blackbyte
Number of observed newly encrypted files	116,007
Encrypted files include	[redacted]

Figure 3: An example of the various stages of the attack on one of the compromise servers being identified by Cyber AI Analyst. Note: this screenshot is from DETECT/Network v.5

As long as threat actors continue to develop new methods of attack, the ability to detect uncategorized threats is required. As demonstrated above, Darktrace's anomaly-based approach lends itself perfectly to detecting these novel or uncategorized threats.

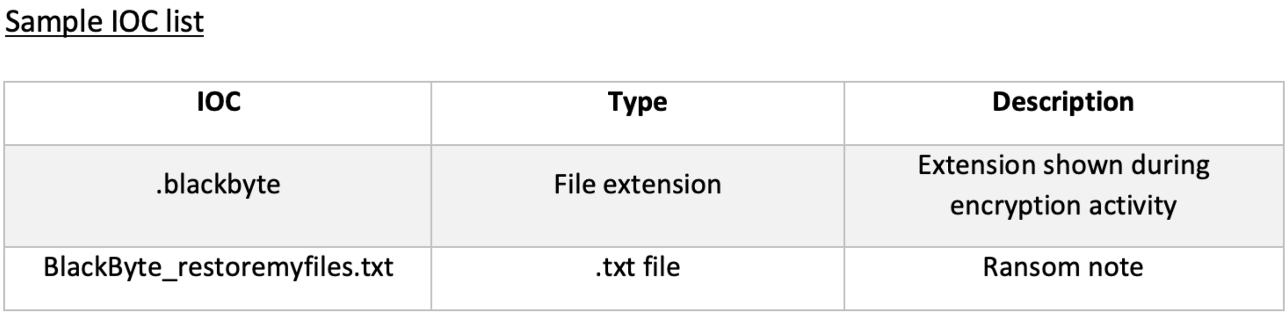
Thanks to Max Heinemeyer for his contributions to this blog.

Appendices

Model Breaches

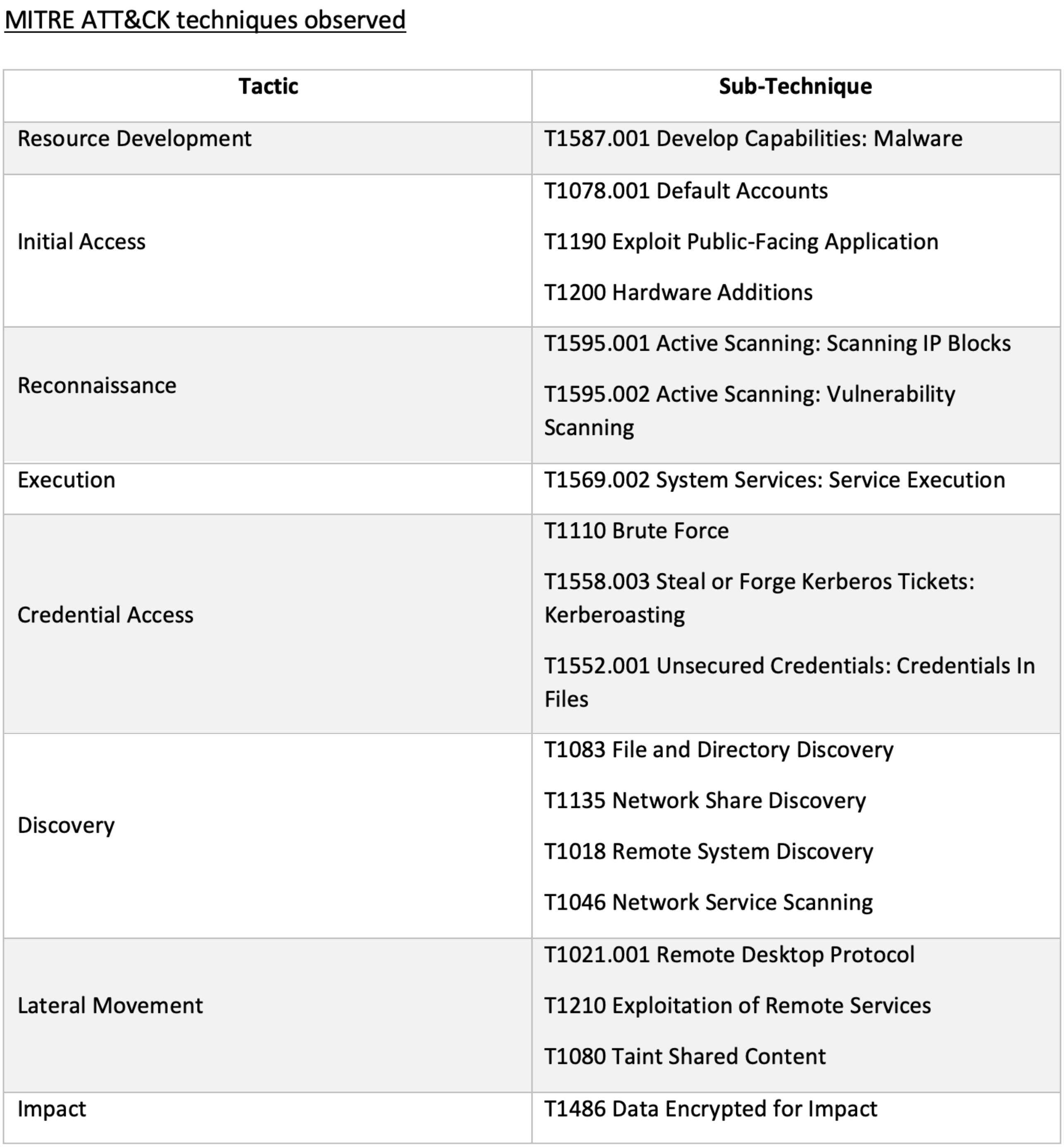
- Anomalous Connection / SMB Enumeration
- Anomalous Connection / Suspicious Activity On High Risk Device
- Anomalous Server Activity / Anomalous External Activity from Critical Network Device
- Compliance / Default Credential Usage
- Device / SMB Session Bruteforce
- Anomalous Connection / Sustained MIME Type Conversion
- Anomalous Connection / Unusual SMB Version 1 Connectivity
- Anomalous File / Internal / Additional Extension Appended to SMB File
- Compliance / Possible Unencrypted Password File on Server
- Compliance / SMB Drive Write
- Compliance / Weak Active Directory Ticket Encryption

- Compromise / Ransomware / Possible Ransom Note Write
- Compromise / Ransomware / Ransom or Offensive Words Written to SMB
- Compromise / Ransomware / SMB Reads then Writes with Additional Extensions
- Compromise / Ransomware / Suspicious SMB Activity
- Device / Attack and Recon Tools in SMB
- Device / Multiple Lateral Movement Model Breaches
- Device / New or Unusual Remote Command Execution
- Device / SMB Lateral Movement
- Device / Suspicious File Writes to Multiple Hidden SMB Shares
- Device / Suspicious Network Scan Activity
- Unusual Activity / Anomalous SMB Read & Write
- Unusual Activity / Anomalous SMB to Server
- User / Kerberos Password Bruteforce



Sample IOC list

IOC	**Type**	**Description**
.blackbyte	File extension	Extension shown during encryption activity
BlackByte_restoremyfiles.txt	.txt file	Ransom note



MITRE ATT&CK techniques observed

Tactic	Sub-Technique
Resource Development	T1587.001 Develop Capabilities: Malware
Initial Access	T1078.001 Default Accounts T1190 Exploit Public-Facing Application T1200 Hardware Additions
Reconnaissance	T1595.001 Active Scanning: Scanning IP Blocks T1595.002 Active Scanning: Vulnerability Scanning
Execution	T1569.002 System Services: Service Execution
Credential Access	T1110 Brute Force T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting T1552.001 Unsecured Credentials: Credentials In Files
Discovery	T1083 File and Directory Discovery T1135 Network Share Discovery T1018 Remote System Discovery T1046 Network Service Scanning
Lateral Movement	T1021.001 Remote Desktop Protocol T1210 Exploitation of Remote Services T1080 Taint Shared Content
Impact	T1486 Data Encrypted for Impact

References

[1] https://www.mandiant.com/resources/zero-days-exploited-2021

[2] https://www.virustotal.com/gui/ip-address/162.243.25.33/relations

[3] https://www.zscaler.com/blogs/security-research/analysis-blackbyte-ransomwares-go-based-variants