Makop Threat Brief

Makop is a ransomware sold by its developers under a Ransomware-as-a-Service (RaaS) model since January 2020. To future proof this strain of ransomware developers use dual encryption with AES256 and RSA1024 to prevent decryption. The source code of Makop is written in C++ and seems based on the Oled ransomware.

Motives

Initially advertised with a decryption cost of $250 in January 2020, the Makop affiliates and developers are financially motivated with ransoms averaging $30,000+. Professional negotiators have historically been successful in bringing Makop ransom costs down around $5,000.

Tactics, Techniques, and Procedures (TTPs)

The majority of Makop ransoms occur from victims engaging with Spearphishing attachments. Ransoms have also been seen after Makop was dropped onto victim's systems by other malware infections.

Once executed Makop uses malicious DLLs and DLL side loading techniques to escalate privilege level on victim systems. After adding itself as a scheduled task at system startup the encryption process begins. Affiliates of Makop provide anonymous email addresses for victims to contact about ransom payment.

Mitre ATT&CK

The following maps Makop's TTPs to MITRE ATT&CK:

Initial Access

- **Phishing: Spearphishing Attachment (T1566.001) -** Makop affiliates actively use Spearphishing campaigns to infect victim systems.

Execution

- **Native API (T1106) -** Makop uses Windows API calls in its execution.

Persistence

- **Scheduled Task/Job (T1053) -** Makop schedules self-execution at Windows startup to maintain persistence.

Privilege Escalation

- **DLL Side-Loading (T1574.002) -** Makop side-loads malicious DLLs into Windows processes to escalate privileges.

Discovery

- **Remote System Discovery (T1018) -** Makop locates network resources using Windows network enumeration functions.

Command and Control

- **Encrypted Channel (T1573) -** Makop has sent HTTP requests via the Windows Error Reporting service.

Impact

- **Inhibit System Recovery (T1490) -** Makop can delete shadow copies to prevent easy restoration post-encryption.
- **Data Encrypted for Impact (T1486) -** Makop can encrypt files and demands a ransom to decrypt the files.

Table of Contents

Mitigations/Defenses

Implementing a strong foundation of security controls is recommended to defend your network from being targeted by Makop affiliates.

The Center for Internet Security (CIS) Controls are a prioritized set of safeguards designed to defend against cyber attacks. The CIS Controls have three tiers, known as Implementation Groups, that build on each other.

The following table maps Makop's MITRE ATT&CK techniques to CIS v8 Safeguards:

MITRE ATT&CK	CIS Safeguards
Phishing: Spearphishing Attachment (T1566.001)	**IG1** 2.3: Address Unauthorized Software 14.1: Establish and Maintain a Security Awareness Program 14.2: Train Workforce Members to Recognize Social Engineering Attacks 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents
Native API (T1106)	**IG1** 2.3: Address Unauthorized Software

Scheduled Task/Job (T1053)	**IG1** 2.1: Establish and Maintain a Software Inventory 2.2: Ensure Authorized Software is Currently Supported 2.3: Address Unauthorized Software 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 8.1: Establish and Maintain an Audit Log Management Process 8.2: Collect Audit Logs 8.3: Ensure Adequate Audit Log Storage 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates 10.3: Disable Autorun and Autoplay for Removable Media 14.1: Establish and Maintain a Security Awareness Program 14.2: Train Workforce Members to Recognize Social Engineering Attacks 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents
DLL Side-Loading (T1574.002)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 7.1: Establish and Maintain a Vulnerability Management Process 7.2: Establish and Maintain a Remediation Process 7.3: Perform Automated Operating System Patch Management 7.4: Perform Automated Application Patch Management

Table of Contents

Process Injection (T1055)	**IG1** 2.1: Establish and Maintain a Software Inventory 2.2: Ensure Authorized Software is Currently Supported 2.3: Address Unauthorized Software 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 8.1: Establish and Maintain an Audit Log Management Process 8.2: Collect Audit Logs 8.3: Ensure Adequate Audit Log Storage 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates 10.3: Disable Autorun and Autoplay for Removable Media 14.1: Establish and Maintain a Security Awareness Program 14.2: Train Workforce Members to Recognize Social Engineering Attacks 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents
File Deletion (T1070.004)	**IG1** 3.1: Establish and Maintain a Data Management Process 3.3: Configure Data Access Control Lists 3.4: Enforce Data Retention 4.1: Establish and Maintain a Secure Configuration Process 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 8.1: Establish and Maintain an Audit Log Management Process 8.2: Collect Audit Logs 8.3: Ensure Adequate Audit Log Storage
Obfuscated Files or Information (T1027)	**IG1** 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates
Rundll32 (T1218.011)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 4.5: Implement and Manage a Firewall on End-User Devices
Masquerading (T1036)	**IG1** 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process

Process Discovery (T1057)	**IG1** 2.1: Establish and Maintain a Software Inventory 2.2: Ensure Authorized Software is Currently Supported 2.3: Address Unauthorized Software 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 8.1: Establish and Maintain an Audit Log Management Process 8.2: Collect Audit Logs 8.3: Ensure Adequate Audit Log Storage 10.1: Deploy and Maintain Anti-Malware Software 10.2: Configure Automatic Anti-Malware Signature Updates 10.3: Disable Autorun and Autoplay for Removable Media 14.1: Establish and Maintain a Security Awareness Program 14.2: Train Workforce Members to Recognize Social Engineering Attacks 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents
Query Registry (T1012)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process
Remote System Discovery (T1018)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process
System Information Discovery (T1082)	**IG1** 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Clipboard Data (T1115)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 6.3: Require MFA for Externally-Exposed Applications 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Access 11.4: Establish and Maintain an Isolated Instance of Recovery Data 14.1: Establish and Maintain a Security Awareness Program 14.3: Train Workforce Members on Authentication Best Practices

Archive Collected Data (T1560)	**IG1** 2.1: Establish and Maintain a Software Inventory 2.2: Ensure Authorized Software is Currently Supported 2.3: Address Unauthorized Software 3.3: Configure Data Access Control Lists 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 4.7: Manage Default Accounts on Enterprise Assets and Software 5.1: Establish and Maintain an Inventory of Accounts 5.2: Use Unique Passwords 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 8.1: Establish and Maintain an Audit Log Management Process 8.2: Collect Audit Logs 8.3: Ensure Adequate Audit Log Storage 9.2: Use DNS Filtering Services 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data 14.1: Establish and Maintain a Security Awareness Program 14.2: Train Workforce Members to Recognize Social Engineering Attacks 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents
Encrypted Channel (T1573)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 4.5: Implement and Manage a Firewall on End-User Devices 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 7.1: Establish and Maintain a Vulnerability Management Process 7.2: Establish and Maintain a Remediation Process 7.3: Perform Automated Operating System Patch Management 7.4: Perform Automated Application Patch Management
Data Encrypted for Impact (T1486)	**IG1** 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Inhibit System Recovery (T1490)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 7.1: Establish and Maintain a Vulnerability Management Process 7.2: Establish and Maintain a Remediation Process 7.3: Perform Automated Operating System Patch Management 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Table of Contents

Detection Opportunities

Makop is dropped and executed either directly from phishing emails or via a secondary malware that has already infected the system. This means defenders must focus on detecting the activities of Makop itself in order to catch its activities before it can encrypt files on endpoints. The below detection opportunities focus on actions taken by Makop ransomware before beginning the encryption process:

Detection Opportunity 1: Shadow Copy and System State Backup Deletion

MITRE ATT&CK: Inhibit System Recovery (T1490)

CIS Control(s): 4.1, 4.2, 4.7, 5.3, 5.4, 7.1, 7.2, 7.3, 11.1, 11.2, 11.3, and 11.4

Red Canary Atomic Red Team Test(s): T1490 - Inhibit System Recovery Test #1, #2, and #3

Before encrypting files on the infected endpoint, Makop will first delete shadow copies and system state backups. This is performed to prevent the user from being able to easily restore their device to a state pre-encryption and not have to pay the ransom demanded by the Makop actor.

Defenders should be able to detect the deletion of these backups by enabling PowerShell Transcription on endpoints they are monitoring. Once enabled, it is recommended to export the transcripts to a remote location which will allow you and your team to monitor PowerShell activity and defend against malicious actors utilizing PowerShell to perform their activities. Searching for the following command within PowerShell logs will allow you to detect potentially malicious pre-encryption activity performed by Makop on your endpoints:

Command: vssadmin delete shadows /all /quiet

Command: wbadmin delete catalog -quiet

Command: wmic shadowcopy delete

References/Appendix/Resources

zdnet.com/article/hackers-exploit-windows-error-reporting-service-in-new-fileless-attack/

trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom.win32.makop.thfbdbo/

provendatarecovery.com/makop-ransomware-recovery/

unit42.paloaltonetworks.com/ransomware-families/

orpheus-cyber.com/blog-makop-raas-campaign-targets-south-korean-entities/

cybergeeks.tech/makop-ransomware/

asec.ahnlab.com/en/27256/

Table of Contents