Cyber Threat Intelligence 02122024

Suspected IP : 23.216.147.64

Shruti Patel

Cyber Security Researcher

Institute of Network Experts

TABLE OF CONTENTS

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

- The investigation centers on an IP address, **23.216.147.64**, which is suspected to host several forms of malware that pose significant threats to organizational security.
- Malware samples associated with this IP address include executables such as win32.EXE and Sharat Service.exe, both identified as malicious through both **YARA** and **Sigma** rule detections.
- These files belong to **advanced malware families**, such as Ibashade, Dronux, and Packedent, and are capable of performing a variety of malicious activities like data exfiltration, persistence establishment, and lateral movement across compromised systems.
- This report provides a **comprehensive analysis** of the malware activity, behavior, and the associated risks, and outlines recommended actions to contain and prevent future infections.

2. DETECTION AND FINDINGS

2.1 Threat Categories

- **Trojan:** A form of malware that disguises itself as a legitimate file or program to trick users into downloading and executing it. Once executed, Trojans may steal sensitive data, enable unauthorized access, or cause damage to the system.
- **Worm:** A self-replicating malware that spreads through networks, often exploiting system vulnerabilities to propagate itself. Worms do not need user interaction to spread.
- **Dropper:** A type of malware that is primarily designed to deliver a second-stage payload (e.g., a virus or Trojan). Droppers may often download additional malicious software without the user's knowledge.

2.2 Malware Family Labels

- **Ibashade:** This malware family is notorious for being stealthy, often using advanced evasion techniques to avoid detection. It is typically used for data theft and reconnaissance activities.
- **Dronux:** Known to target financial institutions and sensitive data, Dronux is frequently used in large scale financial fraud operations, especially in targeted attacks against individuals and corporations.
- **Packedent:** A sophisticated malware family that uses obfuscation techniques, such as packing, to conceal its true nature from traditional security tools. Its goal is usually long-term persistence and control over infected systems.

2.3 Community Reports

1. **Crowdsourced YARA Rules:** YARA rules created by the cybersecurity community have been invaluable in detecting these malware strains. These rules focus on identifying unique patterns and behaviors exhibited by the files.
2. **Crowdsourced Sigma Rules:** Sigma rules for SIEM (Security Information and Event Management) systems have been instrumental in detecting malware activities within corporate environments. These rules help identify and categorize malicious actions on endpoints and network traffic.

2.4 Key Relations

1. **Communicating Files:**

- **win32.EXE:** Detected at a rate of 68 out of 73. This file has been flagged as high-risk due to its association with Trojan behavior, as it can initiate communication with external servers.
- **Sharat Service.exe:** Known for its persistence mechanisms, including modifying registry entries to ensure it starts with the system.

2. **Relationships with Other Threats:** The malware samples communicate with external command-and-control (C2) servers and are involved in actions such as:

- Establishing reverse shell connections.
- Downloading additional malicious payloads.
- Attempting to exploit vulnerabilities to maintain control over infected systems.

3. INDICATORS OF COMPROMISE

IOC 1: Suspicious Executable Running SQL Queries

- **Type:** win32.EXE
- **Description:** This executable file triggers SQL queries that target confidential data stores. This is an indication of potential data exfiltration activities, which may involve unauthorized access to sensitive information.

IOC 2: Base64 Encoded Payload

- **Type:** Sharat Service.exe
- **Description:** This executable is Base64-encoded, suggesting it has been obfuscated to evade detection by traditional security systems. The file serves as a User-Agent for lateral movement across the network, enabling the attacker to move between compromised systems undetected.

4. DETAILED ANALYSIS

4.1 YARA Rule Findings

YARA rules are used to detect patterns in files and processes that are associated with specific malware behaviors. Key findings from the YARA analysis include:

- **Base64 Encoding:** Base64 encoding used by the Sharat Service.exe file is often a method for evading traditional malware detection techniques. This encoding allows the file to bypass security filters and be interpreted as harmless until decoded.
- **Suspicious SQL Query Execution:** The win32.EXE file executes SQL queries aimed at extracting data from sensitive databases. This could be part of a broader data theft or reconnaissance effort.

4.2 Sigma Rule Findings

Sigma rules are designed to work with SIEM systems to detect malicious activity patterns. Key findings include:

1. **High-Severity Detections**

- **Carrotbat Malware Family:** This malware is used primarily as a dropper to deploy additional malicious payloads on infected systems.It can also establish persistent access, allowing attackers to control the system remotely.
- **Syscon Malware Family:** Known for creating a backdoor that allows attackers to maintain access to a system even after initial infection.The malware often communicates with external C2 servers to download additional payloads or exfiltrate data.

- **Oceansalt Malware Family:** This family targets specific geographic regions or industries and is typically used for targeted attacks. Oceansalt often involves heavy data exfiltration techniques and persistence mechanisms.
- **Backswap Trojan:** A particularly dangerous Trojan that arrives as a file dropped by other malware or downloaded from compromised websites. It is often used to monitor financial transactions and steal sensitive financial data, posing significant risks to users' financial security.

2. Low-Severity Detections

- **Suspicious Process Behavior:** Processes started from unusual folders or directories can indicate that the system has been compromised. This activity should be flagged for further investigation.
- **Executable Creation by Executable:** This behavior is often a sign of malware attempting to propagate itself by creating other malicious executables on the system.

5. BEHAVIORAL INSIGHTS

Key Observations

- **Registry Modifications:** The malware attempts to modify system registry entries, particularly under WOW6432Node\CurrentVersion. This is a common tactic used by malware to maintain persistence across system reboots, making it harder to remove.
- **Startup Folder Activity:** Malware files are written to the startup folder, ensuring that they run every time the system starts. This behavior is typical of malware designed to maintain long-term access.
- **Obfuscation Techniques:** Files such as Sharat Service.exe use Base64 encoding.

Malware Impact

- **Data Exfiltration:** The SQL queries observed in win32.EXE are indicative of data theft, potentially exfiltrating sensitive information from internal databases.
- **Financial Fraud:** The Backswap Trojan monitors financial transactions, suggesting that attackers may be attempting to intercept sensitive financial data.
- **Persistence and Propagation:** The malware demonstrates advanced persistence techniques, including modifying the system registry and writing to the startup folder.

6. RECOMMENDATIONS

6.1 Immediate Mitigation Actions

- **Block IP Address:** Add 23.216.147.64 to blocklists across firewalls and IDS/IPS systems to prevent communication with the malicious server.
- **Scan for IOCs:** Use antivirus and EDR solutions to scan for and quarantine files like win32.EXE and Sharat Service.exe.
- **Update Threat Detection Rules:** Integrate updated YARA and Sigma rules into SIEM systems to enhance detection capabilities.
- **Monitor Network Traffic:** Look for unusual Base64-encoded payloads or suspicious User Agent strings in network traffic.

6.2 Long-term Strategies

- **Enhance SIEM Capabilities:** Regularly update and refine SIEM rules to detect new and evolving threats.
- **Endpoint Security:** Deploy endpoint protection solutions such as CrowdStrike or Microsoft Defender to monitor for unusual file creation or modifications.
- **Employee Awareness:** Train employees to recognize phishing emails and other social engineering tactics that could facilitate malware infections.

7. PREVENTION MEASURES

7.1 Immediate Actions to Contain the Threat

- **Block IP Address:** Block all communication to and from the malicious IP 23.216.147.64 at the network perimeter.
- **Scan and Quarantine:** Immediately scan all endpoints for the identified IOCs and quarantine any malicious files.
- **Isolate Affected Systems:** Disconnect any compromised systems to prevent further spread of malware.

7.2 Strengthening Endpoint Security

- **Deploy EDR Solutions:** Use EDR tools to continuously monitor for and block the execution of malicious files.

- **Enforce Application Whitelisting:** Only allow approved applications to run, reducing the risk of executing malicious files.
- **Privilege Management:** Ensure that only authorized users and applications have administrative access to the system.

7.3 Enhancing Network Security

- **Deploy Web Filtering:** Implement DNS filtering to block access to known malicious domains.
- **Secure Network Perimeters:** Configure firewalls to block unauthorized traffic and inspect all outbound traffic for suspicious activity.

7.4 Proactive Monitoring and Threat Detection

- **SIEM Implementation:** Use SIEM systems to aggregate logs and detect malicious behavior based on predefined rules.
- **Deploy IDS/IPS:** Monitor inbound and outbound traffic for unusual patterns indicative of a malware infection.

7.5 Employee Awareness and Training

- **Conduct Regular Security Training:** Provide training on recognizing phishing emails, securing sensitive data, and following security best practices.
- **Simulate Attacks:** Regularly simulate phishing and malware attacks to assess and improve employee responses.

7.6 Long-term Security Strategies

- **Regular Software Patching:** Ensure all systems are kept up to date with the latest security patches to prevent exploitation of vulnerabilities.
- **Threat Intelligence Integration:** Leverage threat intelligence feeds to stay informed about new vulnerabilities and attack methods.
- **Incident Response Plan:** Develop and maintain a comprehensive incident response plan that includes procedures for detecting, responding to, and recovering from malware incidents.

7.7 Advanced Prevention Measures

- **Honeypots and Deception Technology:** Deploy honeypots to detect and divert attackers away from critical systems.

- **Malware Sandboxing:** Use sandbox environments to analyze suspicious files and identify malicious behavior before allowing them to interact with production systems.
- **Zero-Trust Architecture:** Implement a Zero-Trust security model to continuously verify the identity and security posture of users and devices before granting access to resources.

8. CONCLUSION

- The investigation of **IP 23.216.147.64** has revealed multiple forms of malware, including Trojans, worms, and droppers.
- These threats exhibit **sophisticated techniques** such as Base64 encoding, SQL injection, and persistence mechanisms to evade detection.
- By following the recommended immediate actions and strengthening long-term security strategies, organizations can better **protect themselves** from these advanced threats.
- Implementing a **layered security** approach, which combines proactive monitoring, endpoint security, and employee training, is essential to safeguarding sensitive data and maintaining overall network integrity.