***DISCLAIMER**: This advisory is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this advisory or otherwise.*

Executive Summary

This advisory was prepared in collaboration with the National Cybersecurity and Communications Integration Center (NCCIC), United States Secret Service (USSS), Financial Sector Information Sharing and Analysis Center (FS-ISAC), and Trustwave Spiderlabs, acting under contract with the USSS. The purpose of this release is to provide relevant and actionable technical indicators for network defense.

Recent investigations revealed that malicious actors are using publicly available tools to locate businesses that use remote desktop applications. Remote desktop solutions like Microsoft's Remote Desktop,[1] Apple Remote Desktop,[2] Chrome Remote Desktop,[3] Splashtop 2,[4] Pulseway[5], and LogMEIn Join.Me[6] offer the convenience and efficiency of connecting to a computer from a remote location. Once these applications are located, the suspects attempted to brute force the login feature of the remote desktop solution. After gaining access to what was often administrator or privileged access accounts, the suspects were then able to deploy the point-of-sale (PoS) malware and subsequently exfiltrate consumer payment data via an encrypted POST request.

USSS, NCCIC/US-CERT and Trustwave Spiderlabs have been working together to characterize newly identified malware dubbed "Backoff", associated with several PoS data breach investigations. At the time of discovery and analysis, the malware variants had low to zero percent anti-virus detection rates, which means that fully updated anti-virus engines on fully patched computers could not identify the malware as malicious.

Similar attacks have been noted in previous PoS malware campaigns[7] and some studies state that targeting the Remote Desktop Protocol with brute force attacks is on the rise.[8] A *Mitigation and Prevention Strategies* section is included to offer options for network defenders to consider.

Analytic Overview

Capabilities

"Backoff" is a family of PoS malware and has been discovered recently. The malware family has been witnessed on at least three separate forensic investigations. Researchers have identified three primary variants to the "Backoff" malware including 1.4, 1.55 ("backoff", "goo", "MAY", "net"), and 1.56 ("LAST").

These variations have been seen as far back as October 2013 and continue to operate as of July 2014. In total, the malware typically consists of the following four capabilities. An exception is the earliest witnessed variant (1.4) which does not include keylogging functionality. Additionally, 1.55 'net' removed the explorer.exe injection component:

- Scraping memory for track data
- Logging keystrokes
- Command & Control (C2) communication
- Injecting malicious stub into explorer.exe

The malicious stub that is injected into explorer.exe is responsible for persistence in the event the malicious executable crashes or is forcefully stopped. The malware is responsible for scraping memory from running processes on the victim machine and searching for track data. Keylogging functionality is also present in most recent variants of "Backoff". Additionally, the malware has a C2 component that is responsible for uploading discovered data, updating the malware, downloading/executing further malware, and uninstalling the malware. See Figure 1 for a depiction of the process for the malware's execution.

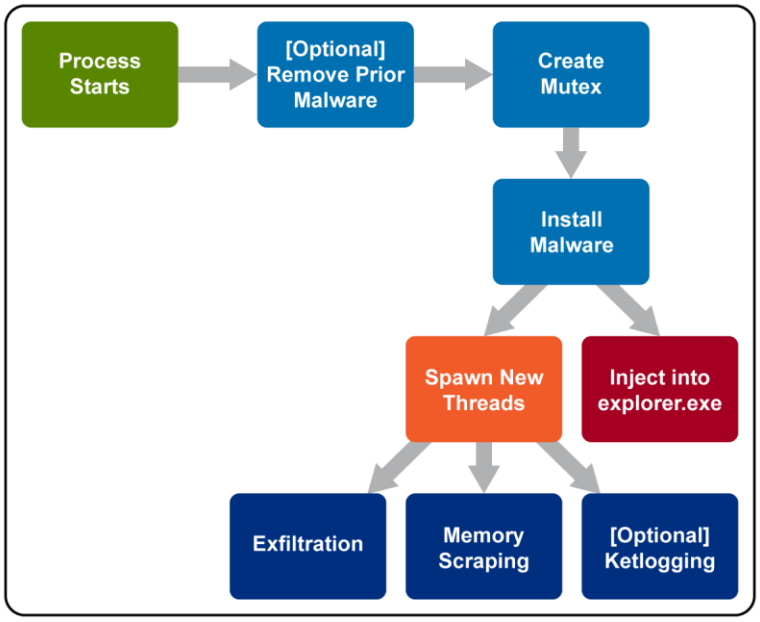

Figure 1: "Backoff" Malware Execution Flow

Variants

Based on compiled timestamps and versioning information witnessed in the C2 HTTP POST requests, "Backoff" variants were analyzed over a seven month period. The five variants witnessed in the "Backoff" malware family have notable modifications, to include:

1.55 "backoff"

- Added Local.dat temporary storage for discovered track data
- Added keylogging functionality
- Added "gr" POST parameter to include variant name
- Added ability to exfiltrate keylog data
- Supports multiple exfiltration domains
- Changed install path
- Changed User-Agent

1.55 "goo"

- Attempts to remove prior version of malware
- Uses 8.8.8.8 as resolver

1.55 "MAY"

- No significant updates other than changes to the URI and version name

1.55 "net"

- Removed the explorer.exe injection component

1.56 "LAST"

- Re-added the explorer.exe injection component
- Support for multiple domain/URI/port configurations
- Modified code responsible for creating exfiltration thread(s)
- Added persistence techniques

Command & Control Communication

All C2 communication for "Backoff" takes place via HTTP POST requests. Note that all data in Figure 2 was generated in a closed sandboxed environment; no legitimate track data is being shown.

As shown in the example, a number of POST parameters are included when this malware makes a request to the C&C server.

Figure 2: HTTP POST Request from Latest Variant (1.56 "LAST")

- op : Static value of '1'
- id : randomly generated 7 character string
- ui : Victim username/hostname
- wv : Version of Microsoft Windows
- gr (Not seen in version 1.4) : Malware-specific identifier
- bv : Malware version
- data (optional) : Base64-encoded/RC4-encrypted data

The 'id' parameter is stored in the following location, to ensure it is consistent across requests:

- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\identifier

If this key doesn't exist, the string will be generated and stored. Data is encrypted using RC4 prior to being encoded with Base64. The password for RC4 is generated from the 'id' parameter, a static string of 'jhgtsd7fjmytkr', and the 'ui' parameter. These values are concatenated together and then hashed using the MD5 algorithm to form the RC4 password. In the above example, the RC4 password would be '56E15A1B3CB7116CAB0268AC8A2CD943 (The MD5 hash of 'vxeyHkSjhgtsd7fjmytkrJosh @ PC123456).

Mitigation and Prevention Strategies

At the time this advisory is released, the variants of the "Backoff" malware family are largely undetected by anti-virus (AV) vendors. However, shortly following the publication of this technical analysis, AV companies will quickly begin detecting the existing variants. It's important to maintain up-to-date AV signatures and engines as new threats such as this are continually being added to your AV solution. Pending AV detection of the malware variants, network defenders can apply indicators of compromise (IOC) to a variety of prevention and detection strategies.[9,10,11] IOCs can be found in *Appendix 1: Technical Malware Analysis*.

The forensic investigations of compromises of retail IT/payment networks indicate that the network compromises allowed the introduction of memory scraping malware to the payment terminals. Information security professionals recommend a defense in depth approach to mitigating risk to retail payment systems. While some of the risk mitigation recommendations are general in nature, the following

strategies provide an approach to minimize the possibility of an attack and mitigate the risk of data compromise:

Remote Desktop Access

- Configure the account lockout settings to lock a user account after a period of time or a specified number of failed login attempts. This prevents unlimited unauthorized attempts to login whether from an unauthorized user or via automated attack types like brute force.[12]
- Limit the number of users and workstation who can log in using Remote Desktop.
- Use firewalls (both software and hardware where available) to restrict access to remote desktop listening ports (default is TCP 3389).[13]
- Change the default Remote Desktop listening port.
- Define complex password parameters. Configuring an expiration time and password length and complexity can decrease the amount of time in which a successful attack can occur.[14]
- Require two-factor authentication (2FA) for remote desktop access.[15]
- Install a Remote Desktop Gateway to restrict access.[16]
- Add an extra layer of authentication and encryption by tunneling your Remote Desktop through IPSec, SSH or SSL.[17,18]
- Require 2FA when accessing payment processing networks. Even if a virtual private network is used, it is important that 2FA is implemented to help mitigate keylogger or credential dumping attacks.
- Limit administrative privileges for users and applications.
- Periodically review systems (local and domain controllers) for unknown and dormant users.

Network Security

- Review firewall configurations and ensure that only allowed ports, services and Internet protocol (IP) addresses are communicating with your network. This is especially critical for outbound (e.g., egress) firewall rules in which compromised entities allow ports to communicate to any IP address on the Internet. Hackers leverage this configuration to exfiltrate data to their IP addresses.
- Segregate payment processing networks from other networks.
- Apply access control lists (ACLs) on the router configuration to limit unauthorized traffic to payment processing networks.
- Create strict ACLs segmenting public-facing systems and back-end database systems that house payment card data.
- Implement data leakage prevention/detection tools to detect and help prevent data exfiltration.
- Implement tools to detect anomalous network traffic and anomalous behavior by legitimate users (compromised credentials).

Cash Register and PoS Security

- Implement hardware-based point-to-point encryption. It is recommended that EMV-enabled PIN entry devices or other credit-only accepting devices have Secure Reading and Exchange of Data (SRED) capabilities. SRED-approved devices can be found at the Payment Card Industry Security Standards website.
- Install Payment Application Data Security Standard-compliant payment applications.
- Deploy the latest version of an operating system and ensure it is up to date with security patches, anti-virus software, file integrity monitoring and a host-based intrusion-detection system.
- Assign a strong password to security solutions to prevent application modification. Use two-factor authentication (2FA) where feasible.
- Perform a binary or checksum comparison to ensure unauthorized files are not installed.

- Ensure any automatic updates from third parties are validated. This means performing a checksum comparison on the updates prior to deploying them on PoS systems. It is recommended that merchants work with their PoS vendors to obtain signatures and hash values to perform this checksum validation.
- Disable unnecessary ports and services, null sessions, default users and guests.
- Enable logging of events and make sure there is a process to monitor logs on a daily basis.
- Implement least privileges and ACLs on users and applications on the system.

Incident Response

- Deploy a Security Information and Event Management (SIEM), a system that serves as a central point for managing and analyzing events from network devices. A SIEM has two primary responsibilities:
    - Aggregates events and logs from network devices and applications
    - Uses intelligence to analyze and uncover malicious behavior on the network
- Offload logs to a dedicated server in a secure location where unauthorized users can't tamper with them.
- Invest in a dedicated incident response team (IRT) that has the knowledge, training and certification to respond to a breach. For more information on IRT training, visit the SANS Institute website.
- Test and document incident response plans to identify and remediate any gaps prior to an attack. Plans should be updated periodically to address emerging threats.

Points of Contact

- For all inquiries pertaining to this product, please contact the NCCIC Duty Officer at NCCIC@hq.dhs.gov or (888) 282-0870. To report an incident, contact US-CERT at soc@us-cert.gov or visit: http://www.us-cert.gov.

- For law enforcement assistance, please contact your local U.S. Secret Service Field Office/Electronic Crimes Task Force (ECTF) or the USSS toll free number at (877) 242-3375. The U.S. Secret Service has taken a lead role in mitigating the threat of financial crimes since the agency's inception in 1865. As technology has evolved, the scope of the U.S. Secret Service's mission has expanded from its original counterfeit currency investigations to also include emerging financial, electronic and cyber crimes. As a component agency within the U.S. Department of Homeland Security, the U.S. Secret Service has established successful partnerships in both the law enforcement and business communities – across the country and around the world – in order to effectively combat financial crimes.

- The FS-ISAC encourages member institutions to report any observed fraudulent activity through the FS-ISAC submission process and login at http://www.fsisac.com/. This reporting can be done with attribution or anonymously and will assist other members and their customer to prevent, detect and respond to similar activity.

Feedback

NCCIC/US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.

Appendix 1: Technical Malware Analysis

The following technical information is intended to allow those potentially affected by similar activity to check their systems for potentially malicious activity. Network indicators (and specifically, IPs) linked to this attack have been redacted due to ongoing law enforcement investigations.

Indicators of Compromise (IOCs)

1.4

Packed MD5: 927AE15DBF549BD60EDCDEAFB49B829E
Unpacked MD5: 6A0E49C5E332DF3AF78823CA4A655AE8
Install Path: %APPDATA%\AdobeFlashPlayer\mswinsvc.exe
Mutexes:
uhYtntr56uisGst
uyhnJmkuTgD
Files Written:
%APPDATA%\mskrnl
%APPDATA%\winserv.exe
%APPDATA%\AdobeFlashPlayer\mswinsvc.exe
Static String (POST Request): zXqW9JdWLM4urgjRkX
Registry Keys:
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\identifier
HKCU\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run\Windows NT Service
User-Agent: Mozilla/4.0
URI(s): /aircanada/dark.php

1.55 "backoff"

Packed MD5: F5B4786C28CCF43E569CB21A6122A97E
Unpacked MD5: CA4D58C61D463F35576C58F25916F258
Install Path: %APPDATA%\AdobeFlashPlayer\mswinhost.exe
Mutexes:
Undsa8301nskal
uyhnJmkuTgD
Files Written:
%APPDATA%\mskrnl
%APPDATA%\winserv.exe
%APPDATA%\AdobeFlashPlayer\mswinhost.exe
%APPDATA%\AdobeFlashPlayer\Local.dat
%APPDATA%\AdobeFlashPlayer\Log.txt
Static String (POST Request): ihasd3jasdhkas
Registry Keys:
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\identifier
HKCU\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run\Windows NT Service
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
URI(s): /aero2/fly.php

1.55 "goo"

Packed MD5: 17E1173F6FC7E920405F8DBDE8C9ECAC
Unpacked MD5: D397D2CC9DE41FB5B5D897D1E665C549
Install Path: %APPDATA%\OracleJava\javaw.exe
Mutexes:
nUndsa8301nskal
nuyhnJmkuTgD
Files Written:
%APPDATA%\nsskrnl
%APPDATA%\winserv.exe
%APPDATA%\OracleJava\javaw.exe
%APPDATA%\OracleJava\Local.dat
%APPDATA%\OracleJava\Log.txt
Static String (POST Request): jhgtsd7fjmytkr
Registry Keys:
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\identifier
HKCU\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run\Windows NT Service
User-Agent:
URI(s): /windows/updcheck.php

1.55 "MAY"

Packed MD5: 21E61EB9F5C1E1226F9D69CBFD1BF61B
Unpacked MD5: CA608E7996DED0E5009DB6CC54E08749
Install Path: %APPDATA%\OracleJava\javaw.exe
Mutexes:
nUndsa8301nskal
nuyhnJmkuTgD
Files Written:
%APPDATA%\nsskrnl
%APPDATA%\winserv.exe
%APPDATA%\OracleJava\javaw.exe
%APPDATA%\OracleJava\Local.dat
%APPDATA%\OracleJava\Log.txt
Static String (POST Request): jhgtsd7fjmytkr
Registry Keys:
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\identifier
HKCU\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run\Windows NT Service
User-Agent:
URI(s): /windowsxp/updcheck.php

1.55 "net"

Packed MD5: 0607CE9793EEA0A42819957528D92B02
Unpacked MD5: 5C1474EA275A05A2668B823D055858D9
Install Path: %APPDATA%\AdobeFlashPlayer\mswinhost.exe
Mutexes:
nUndsa8301nskal
Files Written:
%APPDATA%\AdobeFlashPlayer\mswinhost.exe
%APPDATA%\AdobeFlashPlayer\Local.dat
%APPDATA%\AdobeFlashPlayer\Log.txt
Static String (POST Request): ihasd3jasdhkas9
Registry Keys:

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\identifier
HKCU\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run\Windows NT Service
User-Agent:
URI(s): /windowsxp/updcheck.php

1.56 "LAST"

Packed MD5: 12C9C0BC18FDF98189457A9D112EEBFC
Unpacked MD5: 205947B57D41145B857DE18E43EFB794
Install Path: %APPDATA%\OracleJava\javaw.exe
Mutexes:
nUndsa8301nskal
nuyhnJmkuTgD
Files Written:
%APPDATA%\nsskrnl
%APPDATA%\winserv.exe
%APPDATA%\OracleJava\javaw.exe
%APPDATA%\OracleJava\Local.dat
%APPDATA%\OracleJava\Log.txt
Static String (POST Request): jhgtsd7fjmytkr
Registry Keys:
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\identifier
HKCU\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run\Windows NT Service
HKLM\ SOFTWARE \Microsoft\Windows\CurrentVersion\Run\Windows NT Service
HKCU\SOFTWARE\\Microsoft\Active Setup\Installed Components\{B3DB0D62-B481-4929-888B-49F426C1A136}\StubPath
HKLM\SOFTWARE\\Microsoft\Active Setup\Installed Components\{B3DB0D62-B481-4929-888B-49F426C1A136}\StubPath
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
URI(s): /windebug/updcheck.php

References

[1] Windows Remote Desktop: http://apps.microsoft.com/windows/en-us/app/remote-desktop/051f560e-5e9b-4dad-8b2e-fa5e0b05a480
[2] Apple Remote Desktop: https://www.apple.com/remotedesktop/
[3] Chrome Remote Desktop: https://chrome.google.com/webstore/category/apps?hl=en
[4] Splashtop: http://www.splashtop.com/downloads-all
[5] Windows Pulseway: http://apps.microsoft.com/windows/en-gb/app/pc-monitor/9efc1d1c-6816-48bc-8de7-d4b21a5b3589
[6] Windows Join.me: http://apps.microsoft.com/windows/en-gb/app/join-me/72920ad1-d57c-4b60-b595-a5078859cbc2
[7] Attacker's brute-force POS systems utilizing RDP in global botnet operation. http://www.scmagazine.com/attackers-brute-force-pos-systems-utilizing-rdp-in-global-botnet-operation/article/360156/
[8] Brute force RDP attacks depend on your mistakes: http://www.zdnet.com/brute-force-rdp-attacks-depend-on-your-mistakes-7000031071/
[9] Understanding Indicators of Compromise (IOC): https://blogs.rsa.com/understanding-indicators-of-compromise-ioc-part-i/
[10] Using Indicators of Compromise in Malware Forensics: http://www.sans.org/reading-room/whitepapers/forensics/ioc-indicators-compromise-malware-forensics-34200
[11] Indicators of Compromise: The Key to Early Detection: http://www.tripwire.com/state-of-security/security-data-protection/indicators-of-compromise-the-key-to-earlier-detection-of-breaches/
[12] Configuring Account Lockout: http://technet.microsoft.com/en-us/library/cc737614%28v=ws.10%29.aspx
[13] Securing Remote Desktop for System Administrators: https://security.berkeley.edu/node/94
[14] Account Lockout and Password Concepts: http://technet.microsoft.com/en-us/library/cc780271%28v=ws.10%29.aspx
[15] NIST Guide to Enterprise Telework and Remote Access Security: http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf
[16] Installing RD Gateway: http://technet.microsoft.com/en-us/library/dd983949
[17] Networking and Access Technologies: http://technet.microsoft.com/en-us/network/bb531150
[18] Secure RDS Connections with SSL: http://technet.microsoft.com/en-us/magazine/ff458357.aspx