FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

18 March 2015

Alert Number
A-000053-MW

The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local Cyber Task Force or FBI CyWatch. Press inquiries should be directed to the FBI's National Press Office.

Local Field Offices:
www.fbi.gov/contact-us/field

CyWatch:
Email: cywatch@ic.fbi.gov
Phone: 1-855-292-3937

National Press Office:
Email: npo@ic.fbi.gov
Phone: 202-324-3691

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP:GREEN: The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

Summary

The FBI is providing the following information with HIGH confidence:

The FBI has obtained information regarding one or more groups of cyber actors who have compromised and stolen sensitive business information from US commercial and government networks through cyber espionage. Analysis indicates a significant amount of the computer network exploitation activities emanated from infrastructure located within China. Any activity related to these groups detected on a network should be considered an indication of a compromise requiring extensive mitigation and contact with law enforcement.

Technical Details

The FBI is providing the following information with HIGH confidence:

These groups have been observed across a variety of intrusions leveraging a diverse selection of tools and techniques to attempt to gain initial access to a victim including using VPN credentials acquired during previous intrusions. These groups have also been observed scanning for web-facing devices which are not fully patched and for which there are publically known vulnerabilities. These groups also continue to use malicious documents in spearphishing emails which leverage older vulnerabilities such as CVE-2011-0611 and CVE-2012-0158.

Following such an exploit, such groups have been observed recently using a more sophisticated variant of the 9002 Remote Access Trojan which was previously observed in Operation Aurora and the SunShop Campaign. The most recent variant employed a DLL load order hijacking technique and was named ws2_32.dll on the infected system. The DLL load order hijacking technique enabled the 9002 variant to load and gain persistence on the system when a susceptible application attempted to load the legitimate ws2_32.dll. The 9002 variant, which created a mutex named 'xws2_32', contained the same export functions as the legitimate ws2_32.dll which facilitates the redirection of legitimate API calls. The 9002 variant decoded malicious sections of code at runtime which were not written to disk. The initial beacon was transmitted as a POST request with a dynamic 4 byte XOR key starting at offset 0 that changed with each subsequent beacon and was Base64 encoded prior to transmission. The behavior of this 9002 variant was similar to the 'Diskless 9002 RAT' referenced in open source reporting.

These groups leverage their initial accesses to gain further access to protected information resources on other systems by collecting legitimate credentials or even misusing legitimate certificates introduced into that compromised system or endpoint. In some cases these groups established automated maintenance routines using standard system administration tools to collect and exfiltrate password hashes on a regular schedule without outside intervention. In other cases, specific tools designed to hijack PKI credentials such as the "Sykipot" malware enabled their ability to harvest and misuse legitimate user certificates. See the SANS report at www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-sykipot-smartcard-proxy-variant-33919.

File Information:

Name: 256438747bae78c9101c9a0d4efe5572
MD5: 256438747BAE78C9101C9A0D4EFE5572
Beaconing traffic to: cache.dnsde.com
Details: HOMEUNIX/9002 malware binary encrypted with password "NeverSayDie!"

If the presence of such tools is detected, it should be immediately flagged, given priority for enhanced mitigation and reported to FBI CYWATCH

Recommended Steps for Initial Mitigation

The FBI and NSA recommend the following mitigation measures be taken within the first 72 hours of detection:

Prepare Your Environment for Incident Response

- Establish Out-of-Band Communications methods for dissemination of intrusion response plans and activities, inform NOCs/CERTs according to institutional policy and SOPs
- Maintain and actively monitor centralized host and network logging solutions after ensuring that all devices have logging enabled and their logs are being aggregated to those centralized solutions

- Disable all remote (including RDP & VPN) access until a password change for all accounts has been completed
- Turn on enhanced monitoring functionality with high-powered analytics to detect known security events and changes in adversary behavior.
- Monitor accounts and devices determined to be part of the compromise to prevent reacquisition attempts

Implement core mitigations to prevent continued access to protected information on non-compromised systems (within 72 hours)

- Home users should follow industry-recognized best practices on home systems if they use them to connect to their corporate networks, especially in instances where home use of trusted certificates or other sensitive credentials are required for log-in. Connections from home users or other remote systems involved in credential hijacking should be suspended.
- Activate and update comply-to-connect solutions to ensure that remote connections are properly configured. Ensure the comply-to-connect enforces that AV signatures are up to date and include signatures for PKI credential hijacking malware such as "Sykipot" for all systems.

  (Please see the SANS article at: www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-sykipot-smartcard-proxy-variant-33919)
- Ensure servers containing restricted information that are remotely accessible are properly configured to implement public-key authentication to ensure that expired and/or revoked credentials cannot be used on the network. When public-key authentication is used, ensure that all less secure forms of authentication are disabled.
- Limit issuing soft-certs (including derived or role-based user, as well as infrastructure, application and other non-person) credentials to only operationally necessary use cases. Soft-certs are software certificates where the private key for the certificate resides in software and can be stolen easily by an attacker for reuse. For necessary soft-cert use-cases, deliver PKCS-files and passwords in ways which eliminate unnecessary exposure, by implementing end-to-end TLS protections between the PKI infrastructure and authorized devices. Track all such issuances to any and all devices where the credential could possibly be activated. If there is any indication of compromise of any device containing soft-certs; revoke the certificate for reason of key compromise. Minimize issuance of soft-certs to high risk systems where the likelihood of compromise is high.
- Integrate a centralized analytic to track credentials used to access protected resources. Analytic capabilities similar to those used to detect credit card fraud can be applied to user credentials to

detect fraudulent use, such as credential hijacking. Anomalous access patterns should be investigated to determine if hijacking is occurring. Confirmation of certificate hijacking cases involving hardware-protected PKI credentials with non-exportable private keys (e.g., CAC or PIV) will identify one or more compromised systems, each of which will require remediations. Remediations include blacklisting source IP addresses determined to be part of an adversary's command and control infrastructure and sanitizing compromised endpoints and systems according to these instructions. Any soft-certs installed on a compromised system should be revoked. Hardware-protected PKI credentials used on a compromised system need not be revoked, but should be suspended (marked as invalid during the time of potential adversarial control) until the compromised system has been remediated. Once the compromised endpoint or system has been remediated, the user's PIN should be replaced. If the user is held accountable for accesses, the impacted credentials could be revoked.

Implement core mitigations to prevent re-exploitation of any compromised system (within 72 hours)

- For any account used on a compromised system, reset the password and associated internal NT hashes (especially for smart-card logon accounts that do not have passwords), Kerberos Tickets, and other persistent single-sign-on mechanisms.
- **If the network authentication infrastructure (e.g., Active Directory) was compromised, implement a network-wide password reset on the compromised network (preferably with local host access only, no remote changes allowed) to include:**
    - All domain accounts (especially high-privileged administrators)
    - Local Accounts
    - Machine and System Accounts
    - Service Accounts
    - For all accounts, including those using smart-card logon or one-time password systems, reset the internal NT hashes, Kerberos Tickets, and other persistent single-sign-on mechanisms.
- Use of privileged administrator accounts for high-risk activities, such as web browsing and e-mail, should be scrutinized, blocked when possible, and discouraged in all other instances.
- Remote access for privileged accounts and functions should be suspended. Use of privileged accounts and administrative functionality should be restricted to only trusted, secured, and monitored systems.
- Establish enhanced monitoring of any system or component suspected to be infected with malware.

- Ensure all impacted systems are rebuilt from a known good image, with up-to-date patches and security configurations.

General mitigations to prevent exploitation:

Patch systems for critical vulnerabilities:

A patch management process that regularly patches vulnerable software remains a critical component in raising the difficulty of intrusions for cyber operators. While a few adversaries use zero-day exploits to target victims, many adversaries still target known vulnerabilities for which patches have been released, capitalizing on slow patch processes and risk decisions by network owners not to patch certain vulnerabilities or systems. At this time, a few of these more widely targeted vulnerabilities are: CVE-2014-0322, CVE-2013-3893, and CVE-2012-0158. While watching for infections from the malware families detailed above, ensure that you are patched against older vulnerabilities commonly exploited by cyber operators, such as CVE-2012-0158. Prioritize timely patching especially for higher risk systems, such as outward-facing devices, including web services, mail services, VPN services, and firewalls.

Mitigations for remote access:

Allowing users to work from home exacerbates the potential for credential hijacking. User managed systems are often less well maintained than corporately managed resources and users typically practice much riskier behavior on their home systems where corporate appropriate use policies do not apply. Also, the ability of an enterprise to apply mitigations to user managed systems is limited. As thin client solutions become more affordable, agencies should consider deploying them as enterprise managed endpoints. For entities that support access to official systems via user managed endpoints, following NSA's 'Best practices for securing a home network' should be encouraged. In particular, virus definitions should be up-to-date and should protect against malware known to support credential hijacking. However, it might be difficult for an enterprise to enforce the adherence for user managed equipment. Consider providing an assured boot mechanism for official use of user managed systems, such as the Lightweight Portable Security (LPS-Public at http://spi.dod.mil/lipose.htm), and require its use for remote access.

Access points for remote access should include a comply-to-connect inspection that validates corporately managed endpoints as up-to-date, and enforces the use of a current secure boot mechanism for user managed endpoints. The landing point for remote accesses should be sandboxed and allow a limited reach into corporate resources based on a restrictive policy commensurate with the threat environment. Administrative privileges should not be supported via remote access.

Mitigations for protected resources:

Resources that are not approved for public release need to be protected so that only authorized users are allowed access, and authorized users who access the resources are held accountable for their actions. At a minimum, users must be authenticated using credentials issued by a trusted certification authority operating under an acceptable certificate policy and/or practice statement. Proper implementation of the authentication mechanism is required to ensure that the validity mechanisms supported by the PKI are enforced. When feasible, smart-card logon should be required for all user accounts, especially for privileged accounts. Security Technical Implementation Guides (STIGs) and additional public key enabling guidance for implementing PKI enforcement for common web servers are available on DISA's IASE page. The server configuration should be tested, both using the STIG checklist, as well as via an independent web scanning tool. The tool should specifically attempt to use expired and revoked certificates issued by a trusted PKI, and see that those accesses are denied.

Privileged accounts should be protected and isolated from exposure. Smart-card logon for privileged accounts should be required, and should either ensure that they can only be activated from dedicated privileged workstations, or should use separate credentials than those issued for regular users (non-privileged accounts).

Access control for restricted resources should be based on authenticated identities, but need to consider more than just authentication. Just because a user was able to login somewhere on the network does not mean that the user should have access to all the sensitive data and resources on the network. Closed deployments of public key infrastructures have been used to create 'default' access control policies based solely on authentication, but these PKI deployments can take on complex trust relationships through the use of cross-certificates and bridge certificate authorities. These trust relationships can change over time allowing many more users on the network, and might not reflect the intended access policy for protected resources. Granular access policies are recommended for any non-public resource.

In large enterprises, simple access control lists can become difficult to manage. Role-based, or even attribute based access control mechanisms can more easily support a large dynamic user environment.