Pond Loach delivers BadCake malware

accenture.com/us-en/blogs/blogs-pond-loach-delivers-badcake-malware

Share

During 2018, iDefense observed several events likely attributed to the POND LOACH (aka APT32 and OceanLotus) threat group, an adversary that has likely been active since 2013. This group is allegedly behind an intrusion event into at least one organization operating in the hospitality sector in 2018, according to recent reporting by security researchers at CrowdStrike.[1]

About POND LOACH

iDefense has moderate confidence that POND LOACH has been operating in or near Vietnam and is possibly supported by the Vietnamese government. This assessment is based upon open- and closed-source information pertaining to prior targeting of foreign governments, journalists, dissidents and private sector organizations operating across numerous industries with significant business interests in Vietnam, with these entities including countries in Southeast Asia, such as the Philippines, Laos and Cambodia (e.g. Association of Southeast Asian Nations [ASEAN]).

POND LOACH appears to be well funded, as evidenced by its developed variety of custom backdoors to target Windows and Mac operating systems, as previously noted by security researchers at Palo Alto Networks[2] and ESET.[3] One of these custom backdoors that iDefense has continued to track is known as BadCake. This backdoor is commonly dropped by either an SFX or an exploit document (e.g. Microsoft Corp. Word or PDF file).

Some of this backdoor's observed capabilities include:

- Arbitrary file, process and registration creation
- Fingerprinting the local machine
- Running arbitrary shellcode

Once dropped, it is usually divided into multiple components in order to be side-loaded, in a fashion similar to other remote access tools including PlugX[4] and NetTraveler.[5] Several examples of BadCake abusing legitimate, signed executables to carry out DLL side-loading techniques include the following:

- Symantec file rastlsc.exe to import the rastls.dll malware file
- McAfee file mcoemcpy.exe to import the McUtil.dll malware file

POND LOACH tactics and techniques

iDefense analysts have used the MITRE ATT&CK[6] framework to map the observed POND LOACH tactics and techniques shown below:

- Initial Access
  - **Drive-by Compromise**: Watering hole attacks via use of malicious JavaScript to profile websites
  - **Spear Phishing Attachment:** Spear phishing e-mails containing malicious documents (RTF, Word, Excel) with embedded executable content
  - **Valid Accounts:** Use of legitimate local admin account credentials
- Execution
  - **PowerShell**: Use of PowerShell-based tools and shellcode loaders for execution
  - **Regsvr32:** Creates a scheduled task that uses regsvr32.exe to execute a COM scriptlet that dynamically downloads a backdoor and injects it into memory
  - **Scheduled Task:** Use of scheduled tasks to persist on victim systems, including BadCake creating a scheduled task to execute the executable that sideloads the DLL at a set time or interval each day.
  - **Signed Script Proxy Execution:** Use of PubPrn.vbs within execution scripts to execute malware, possibly bypassing defenses
  - **User Execution:** Attempts to lure users to execute a malicious dropper contained within spear-phishing attachments
- Persistence
  - **New Service**: Creates a Windows service to establish persistence
  - **Web Shell:** Use of Web shells to maintain access to victim websites

- Privilege Escalation
  - **Exploitation for Privilege Escalation**: Use of CVE-2016-7255 vulnerability to escalate privileges
- Defense Evasion
  - **Binary Padding**: Inclusion of garbage code to mislead anti-malware software and researchers
  - **DLL Side-Loading**: Use of genuinely signed executables from Symantec Corporation and McAfee, LLC to load malicious DLL files, such as with BadCake, when the Symantec executable (rastlsc.exe) is used to load a malicious DLL file (rastls.dll) from the same directory
  - **Indicator Removal on Host**: Clears select event log entries
  - **Masquerading**: Use of hidden or non-printing characters to help masquerade filenames on a system, such as appending a Unicode no-break space character to a legitimate service name
  - **Obfuscated Files or Information**: Use of Invoke-Obfuscation framework to obfuscate actor's PowerShell; also performs other forms of code obfuscation
  - **Timestomp**: Use of a scheduled task named "Scheduled Defrags" with a backdated task creation timestamp of June 2, 2016
- Credential Access
  - **Credential Dumping**: Use of Mimikatz to dump stolen system and user credentials
- Discovery
  - **System Information Discovery**: Collects the victim operating system version and computer name
  - **System Owner/User Discovery**: Collects the victim's username
- Lateral Movement
  - **Application Deployment Software**: Compromises McAfee ePolicy Orchestrator (ePO) to move laterally by distributing malware as a software deployment task
  - **Remote File Copy**: Adds JavaScript to victim websites to download additional frameworks that profile and compromise website visitors
- Collection
  - **Automated Collection**: Ability to fingerprint the local machine
- Exfiltration
  - **Exfiltration over Command-and-Control (C2) Channel**: Use of domain generation algorithm (DGA) to create subdomains for C2 servers that are hardcoded into the malware

- C2
    - **Commonly Used Port**: Use of port 80 for C2 communications
    - **Uncommonly Used Port:** Use of port 25123 for C2 communications
    - **Standard Application Layer Protocol:** Use of HTTP protocol for C2 communications; use of JavaScript that communicates over HTTP or HTTPS to attacker-controlled domains to download additional frameworks
    - **Custom C2 Protocol**: Use of a custom TCP protocol, with which the adversary is able to filter who receives the real C2 address by ensuring each sample generates a unique domain name system (DNS) request based on profile data extracted from the host; use of Cobalt Strike malleable C2 functionality to blend in with network traffic

Looking forward

In recent years, POND LOACH actors have continued to use TTPs such as strategic website compromise (SWC) and spear-phishing attacks to deliver custom website profiling tools and malware backdoors. The likely objective for this group appears to be infiltrating the digital assets of foreign public- and private-sector organizations with significant interests in Vietnam to steal intellectual property and confidential business information that may benefit Vietnamese state entities. iDefense analysts believe that this group will continue to be active into next year and that it will re-tool its arsenal as needed to avoid network defense mechanisms.

Download the full article [PDF].

If you have any questions about POND LOACH or would like to know more about the verticals this group has previously targeted or more about its custom malware arsenal, please reach out to the Accenture Security Cyber Defense Services team at idefense@accenture.com

Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do

not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. It is subject to change. Accenture provides the information on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report.

Copyright © 2020 Accenture. All rights reserved. Accenture, its logo, and High Performance Delivered are trademarks

---

[1] https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018OverwatchReport.pdf
[2] https://researchcenter.paloaltonetworks.com/2017/06/unit42-new-improved-macos-backdoor-oceanlotus/
[3] https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf
[4] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-dll-sideloading.pdf
[5] https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests
[6] https://attack.mitre.org

Accenture Cyber Threat Intelligence