Live off the Land? How About Bringing Your Own Island? An Overview of UNC1945

fireeye.com/blog/threat-research/2020/11/live-off-the-land-an-overview-of-unc1945.html

Through Mandiant investigation of intrusions, the FLARE Advanced Practices team observed a group we track as UNC1945 compromise managed service providers and operate against a tailored set of targets within the financial and professional consulting industries by leveraging access to third-party networks (see this blog post for an in-depth description of "UNC" groups).

UNC1945 targeted Oracle Solaris operating systems, utilized several tools and utilities against Windows and Linux operating systems, loaded and operated custom virtual machines, and employed techniques to evade detection. UNC1945 demonstrated access to exploits, tools and malware for multiple operating systems, a disciplined interest in covering or manipulating their activity, and displayed advanced technical abilities during interactive operations.

Mandiant discovered and reported to Oracle CVE-2020-14871, which was addressed in Oracle's October 2020 Critical Patch Update. Mandiant recommends staying current on all current patch updates to ensure a high security posture. We will discuss this vulnerability in greater detail in a follow up blog post.

UNC1945 Attack Lifecycle

The threat actor demonstrated experience and comfort by utilizing unique tactics, techniques and procedures (TTPs) within Unix environments, demonstrating a high level of acumen in conjunction with ease of operability in Microsoft Windows operating systems. They were successful navigating multiple segmented networks and leveraging third-party access to extend operations well beyond the initial victim. Furthermore, UNC1945 operated from several virtual machines pre-configured with post-exploitation tools in addition to their custom toolset to evade detection and forensics.

Initial Compromise

In late 2018, UNC1945 gained access to a Solaris server and installed a backdoor we track as SLAPSTICK in order to capture connection details and credentials to facilitate further compromise. The SSH service of this server was exposed to the internet at the time, the same time we observed first evidence of threat activity. Unfortunately, due to insufficient available evidence, the next indication of activity was in mid-2020 at which time a different Solaris server was observed connecting to the threat actor infrastructure. This indicates a dwell time of approximately 519 days based on recovered artifacts.

- Although we were unable to determine how the late-2018 initial access was accomplished, we did observe successful UNC1945 SSH connections directly to the victim Solaris 10 server, since the SSH service was exposed directly to the internet at the time.

- In mid-2020, we observed UNC1945 deploy EVILSUN—a remote exploitation tool containing a zero-day exploit for CVE-2020-14871—on a Solaris 9 server. At the time, connections from the server to the threat actor IP address were observed over port 8080.
    - Mandiant discovered and reported CVE-2020-14871, a recently patched vulnerability in the Oracle Solaris Pluggable Authentication Module (PAM) that allows an unauthenticated attacker with network access via multiple protocols to exploit and compromise the operating system.
    - According to an April 2020 post on a black-market website, an “Oracle Solaris SSHD Remote Root Exploit” was available for approximately $3,000 USD, which may be identifiable with EVILSUN.
    - Additionally, we confirmed a Solaris server exposed to the internet had critical vulnerabilities, which included the possibility of remote exploitation without authentication.

Establish Foothold and Maintain Persistence

The threat actor used a Solaris Pluggable Authentication Module backdoor we refer to as SLAPSTICK to establish a foothold on a Solaris 9 server. This facilitated user access to the system with a secret hard-coded password and allowed the threat actors to escalate privileges and maintain persistence (see Figure 1).

```
• Log –font –unix | /usr/lib/ssh/sshd sshd kbdint - can <Encoded Password> <IP
  REDACTED> Magical Password
• auth.info | sshd[11800]: [ID 800047 auth.info] Accepted keyboard-interactive for
  root from <IP REDACTED> port 39680 ssh2
• auth.notice | su: [ID 366847 auth.notice] ‘su root’ - succeeded for netcool on
  /dev/pts/31
```

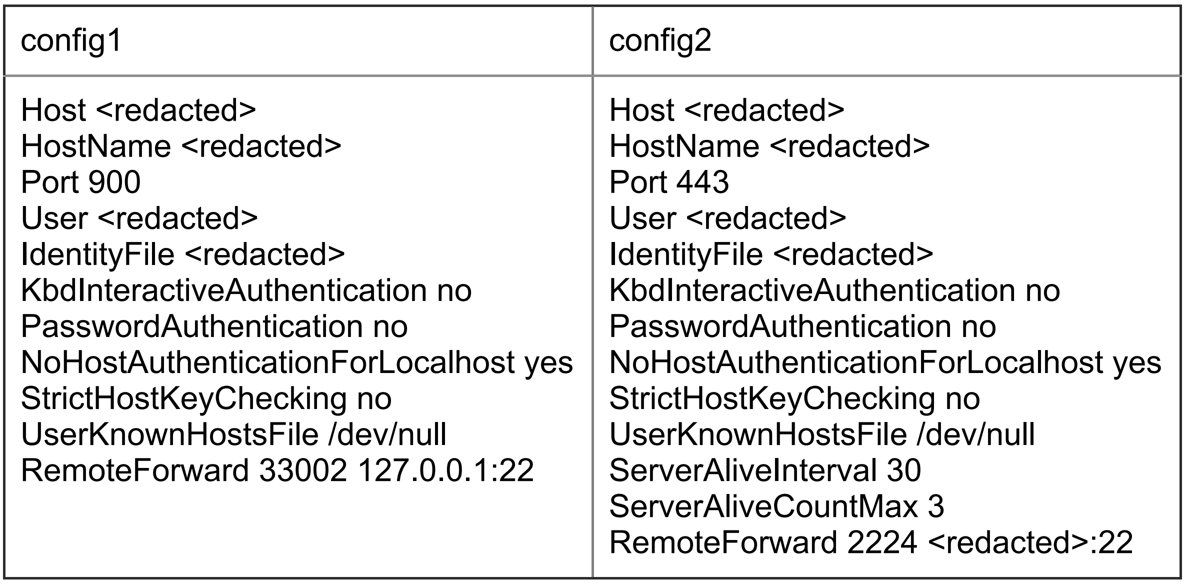
Figure 1: SLAPSTICK logs

At the initial victim, UNC1945 placed a copy of a legitimate pam_unix.so file and SLAPSTICK in the /lib64/security folder. A day later, the threat actor positioned a custom Linux backdoor, which Mandiant named LEMONSTICK, on the same workstation. LEMONSTICK capabilities include command execution, file transfer and execution, and the ability to establish tunnel connections. (see Figure 2).

```
• FileItem:changed | /usr/lib64/security/pam_unix,so [57720]
• Audit log | [audit_type: USER_END] user pid=10080 uid=0 auid=0 msg='PAM:
  session close acct=root" : exe="/usr/sbin/sshd" (hostname=1.239.171.32,
  addr=1.239.171.32, terminal=ssh res=success)'"
• FileItem:Accessed | /var/tmp/.cache/ocb_static
```

Figure 2: UNC1945 emplacement of SLAPSTICK

UNC1945 obtained and maintained access to their external infrastructure using an SSH Port Forwarding mechanism despite the host lacking accessibility to the internet directly. SSH Port Forwarding is a mechanism implemented in SSH protocol for transporting arbitrary networking data over an encrypted SSH connection (tunneling). This feature can be used for adding encryption to legacy applications traversing firewalls or with malicious intent to access internal networks from the the internet. The UNC1945 configurations we observed are similarly structured with respect to the host alias, specified options, and option order (see Figure 3).



config1	config2
Host <redacted> HostName <redacted> Port 900 User <redacted> IdentityFile <redacted> KbdInteractiveAuthentication no PasswordAuthentication no NoHostAuthenticationForLocalhost yes StrictHostKeyChecking no UserKnownHostsFile /dev/null RemoteForward 33002 127.0.0.1:22	Host <redacted> HostName <redacted> Port 443 User <redacted> IdentityFile <redacted> KbdInteractiveAuthentication no PasswordAuthentication no NoHostAuthenticationForLocalhost yes StrictHostKeyChecking no UserKnownHostsFile /dev/null ServerAliveInterval 30 ServerAliveCountMax 3 RemoteForward 2224 <redacted>:22

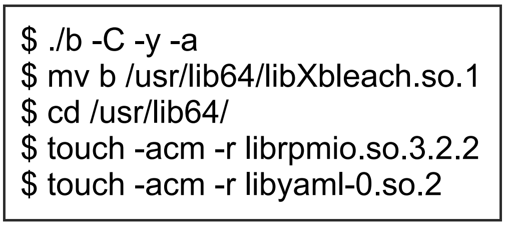
Figure 3: SSH config files used by UNC1945 at different incidents

As part of this multi-stage operation, UNC1945 dropped a custom QEMU Virtual Machine (VM) on multiple hosts, which was executed inside of any Linux system by launching a ‘start.sh’ script. The script contained TCP forwarding settings that could be used by the threat actor in conjunction with the SSH tunnels to give direct access from the threat actor VM to the command and control server to obfuscate interaction with customer infrastructure. The VM was running a version of the Tiny Core Linux OS with pre-loaded scripts and tools. Also, we analyzed the Virtual Machine file system timestamps, which coincided with UNC1945's overall operational timeline.

The VM contained numerous tools such as network scanners, exploits and reconnaissance tools. Tiny Core Linux pre-loaded tools included Mimikatz, Powersploit, Responder, Procdump, CrackMapExec, PoshC2, Medusa, JBoss Vulnerability Scanner and more.

Efforts to decrease operational visibility included placing tool and output files within temporary file system mount points that were stored in volatile memory. Additionally, UNC1945 used built-in utilities and public tools to modify timestamps and selectively manipulate Unix log files.

UNC1945 employed anti-forensics techniques with the use of a custom ELF utility named LOGBLEACH. The actor used built-in Linux commands to alter the timestamps of files and directories and used LOGBLEACH to clean logs to thwart forensic analysis, as seen in Figure 4.



```
$ ./b -C -y -a
$ mv b /usr/lib64/libXbleach.so.1
$ cd /usr/lib64/
$ touch -acm -r librpmio.so.3.2.2
$ touch -acm -r libyaml-0.so.2
```

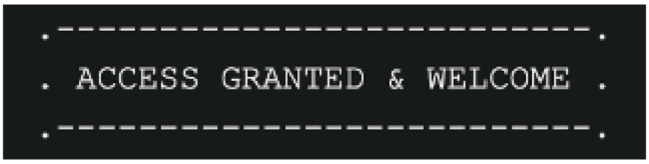
Figure 4: LOGBLEACH

To further obfuscate activity, a Linux ELF packer named STEELCORGI was executed in memory on the Solaris system. The malware contains various anti-analysis techniques, including anti-debugging, anti-tracing, and string obfuscation. It uses environment variables as a key to unpack the final payload.

Escalate Privileges and Lateral Movement

After successfully establishing a foothold, UNC1945 collected credentials, escalated privileges, and successfully moved laterally through multiple networks.

UNC1945 obtained credentials via SLAPSTICK and open source tools such as Mimikatz, which enabled easy lateral movement throughout networks to obtain immediate access to other segments of the network and third-party environments. Stolen credentials collected by SLAPSTICK were used to traverse the customer network via SSH and deploy SLAPSTICK to additional hosts. After successfully authenticating, SLAPSTICK displays a welcome message, as seen in Figure 5.



```
.-------------------------.
. ACCESS GRANTED & WELCOME .
.-------------------------.
```

Figure 5: SLAPSTICK backdoor welcome banner

UNC1945 used ProxyChains to download PUPYRAT, an open source, cross-platform multi-functional remote administration and post-exploitation tool mainly written in Python.

At one target, the threat actor used a virtual machine to initiate a brute-force of SSH targeting Linux and HP-UX endpoints. Beginning with seemingly random usernames and shifting to legitimate Linux and Windows accounts, the threat actor successfully established SSH connections on a Linux endpoint. After successfully escalating privileges on an HP-UX endpoint and a Linux endpoint, UNC1945 installed three backdoors: SLAPSTICK, TINYSHELL, and OKSOLO.

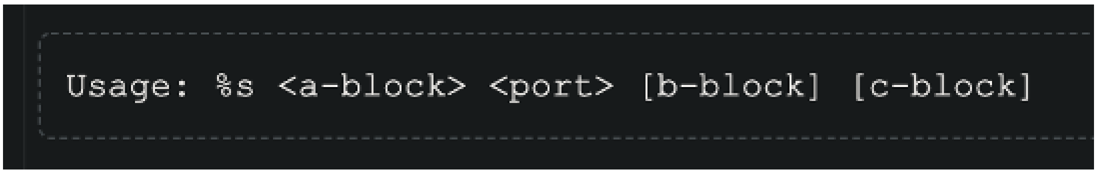
We observed UNC1945 use IMPACKET with SMBEXEC in a Microsoft Windows environment to execute commands remotely without the need to upload a payload to the target. SMBEXEC allows the threat actor to operate like PsExec, but without using RemComSvc. There are two main modes of using this tool that benefits attackers. Share mode allows the specification of a share that everything will be executed through. Server mode permits the output of the executed commands to be sent back by the target machine into a locally shared folder.

At one victim, we observed UNC1945 moving laterally via Remote Desktop Protocol (RDP) to a Windows server before viewing the Server Manager Panel, viewing and modifying RDP-related system firewall rules and checking the application settings of two endpoint security services.

Internal Reconnaissance

Mandiant investigations found that the threat actor maintains various tools to interact with victim networks. In addition to custom tools, the UNC1945 VMs contained various tools (e.g. network scanners, exploits and reconnaissance; see Associated Tools and Malware section).

In some intrusions, UNC1945 employed a SPARC executable identified as a reconnaissance tool. Based on publicly available information, this executable could be referred to as Luckscan or BlueKeep, the latter of which is part of the BKScan toolkit (see Figure 6).



```
Usage: %s <a-block> <port> [b-block] [c-block]
```

Figure 6: SPARC executable recon tool command line used by the threat actor

According to open sources, BlueKeep, aka “bkscan” scanner, works both unauthenticated and authenticated (i.e. when Network Level Authentication is enabled). BlueKeep (CVE-2019-0708) is a security vulnerability that was discovered in Microsoft's Remote Desktop Protocol (RDP) implementation, which allows for the possibility of remote code execution.

Complete Mission

Despite this multi-staged operation, Mandiant did not observe evidence of data exfiltration and was unable to determine UNC1945's mission for most of the intrusions we investigated. In at least one case, we observed ROLLCOAST ransomware deployment in the final phase of the threat actor activity, but Mandiant didn’t attribute this activity to UNC1945. At this time, it is likely that access to the victim environment was sold to another group.

Conclusion

The ease and breadth of exploitation in which UNC1945 conducted this campaign suggests a sophisticated, persistent actor comfortable exploiting various operating systems, and access to resources and numerous toolsets. Given the aforementioned factors, use of zero-day exploits and virtual machines, and ability to traverse multiple third-party networks, Mandiant expects this motivated threat actor to continue targeted operations against key industries while taking advantage of operating systems that likely have inadequate security visibility.

Associated Tools and Malware Families

EVILSUN is a remote exploitation tool that gains access to Solaris 10 and 11 systems of SPARC or i386 architecture using a vulnerability (CVE-2020-14871) exposed by SSH keyboard-interactive authentication. The remote exploitation tool makes SSH connections to hosts passed on the command line. The default port is the normal SSH port (22), but this may be overridden. EVILSUN passes the banner string SSH-2.0-Sun_SSH_1.1.3 over the connection in clear text as part of handshaking.

LEMONSTICK is a Linux executable command line utility with backdoor capabilities. The backdoor can execute files, transfer files, and tunnel connections. LEMONSTICK can be started in two different ways: passing the \`-c\` command line argument (with an optional file) and setting the 'OCB' environment variable. When started with the \`-c\` command line argument, LEMONSTICK spawns an interactive shell. When started in OCB mode, LEMONSTICK expects to read from STDIN. The STDIN data is expected to be encrypted with the blowfish algorithm. After decrypting, it dispatches commands based on the name —for example: 'executes terminal command', 'connect to remote system', 'send & retrieve file', 'create socket connection'.

LOGBLEACH is an ELF utility that has a primary functionality of deleting log entries from a specified log file(s) based on a filter provided via command line. The following log files are hard coded in the malware, but additional log paths may be specified:

- /var/run/utmp
- /var/log/wtmp
- /var/log/btmp
- /var/log/lastlog
- /var/log/faillog
- /var/log/syslog
- /var/log/messages
- /var/log/secure
- /var/log/auth.log

OKSOLO is a publicly available backdoor that binds a shell to a specified port. It can be compiled to support password authentication or dropped into a root shell.

OPENSHACKLE is a reconnaissance tool that collects information about logged-on users and saves it to a file. OPENSHACKLE registers Windows Event Manager callback to achieve persistence.

ProxyChains allows the use of SSH, TELNET, VNC, FTP and any other internet application from behind HTTP (HTTPS) and SOCKS (4/5) proxy servers. This "proxifier" provides proxy server support to any application.

PUPYRAT (aka Pupy) is an open source, multi-platform (Windows, Linux, OSX, Android), multi-function RAT (Remote Administration Tool) and post-exploitation tool mainly written in Python. It features an all-in-memory execution guideline and leaves very low footprint. It can communicate using various transports, migrate into processes (reflective injection), and load remote Python code, Python packages and Python C-extensions from memory.

STEELCORGI is a packer for Linux ELF programs that uses key material from the executing environment to decrypt the payload. When first starting up, the malware expects to find up to four environment variables that contain numeric values. The malware uses the environment variable values as a key to decrypt additional data to be executed.

SLAPSTICK is a Solaris PAM backdoor that grants a user access to the system with a secret, hard-coded password.

TINYSHELL is a lightweight client/server clone of the standard remote shell tools (rlogin, telnet, ssh, etc.), which can act as a backdoor and provide remote shell execution as well as file transfers.

Detections

- FE_APT_Trojan_Linux_STEELCORGI_1
- FE_APT_Trojan_Linux_STEELCORGI_2
- FE_HackTool_Linux64_EVILSUN_1
- FE_HackTool_Linux_EVILSUN_1
- HackTool.Linux.EVILSUN.MVX
- HXIOC UUID: e489ce60-f315-4d1a-a888-77782f687eec
- EVILSUN (FAMILY) 90005075FE_Trojan_Linux_LEMONSTICK_1
- FE_APT_Tool_Win32_OPENSHACKLE_1
- FE_APT_Tool_Win_OPENSHACKLE_1
- HXIOC UUID: 4a56fb0c-6134-4450-ad91-0f622a92701c
- OPENSHACKLE (UTILITY) 90005006
- FE_APT_Backdoor_Linux64_SLAPSTICK_1
- FE_APT_Backdoor_Linux_SLAPSTICK_1
- FE_Backdoor_Win_PUPYRAT_1
  FE_APT_Pupy_RAT
- FE_Ransomware_Win64_ROLLCOAST_1
- FE_Ransomware_Win_ROLLCOAST_1
- HXIOC, 45632ca0-a20b-487f-841c-c74ca042e75a; ROLLCOAST RANSOMWARE (FAMILY)
- Ransomware.Win.ROLLCOAST.MVX

Hashes

- d5b9a1845152d8ad2b91af044ff16d0b (SLAPSTICK)
- 0845835e18a3ed4057498250d30a11b1 (STEELCORGI)
- 6983f7001de10f4d19fc2d794c3eb534
- 2eff2273d423a7ae6c68e3ddd96604bc
- d505533ae75f89f98554765aaf2a330a
- abaf1d04982449e0f7ee8a34577fe8af

Netblocks

- 46.30.189.0/24
- 66.172.12.0/24

ATT&CK Tactic Category	Techniques
Initial Access	T1133 External Remote Services T1190 Exploit Public-Facing Application
Execution	T1059 Command and Scripting Interpreter T1059.001 PowerShell T1064 Scripting
Persistence	T1133 External Remote Services
Lateral Movement	T1021.001 Remote Desktop Protocol T1021.004 SSH
Defense Evasion	T1027 Obfuscated Files or Information T1070.004 File Deletion T1070.006 Timestomp T1064 Scripting T1553.002 Code Signing
Discovery	T1046 Network Service Scanning T1082 System Information Discovery T1518.001 Security Software Discovery
Lateral Movement	T1021.001 Remote Desktop Protocol T1021.004 SSH

Command and Control	T1071 Application Layer Protocol T1090 Proxy T1105 Ingress Tool Transfer T1132.001 Standard Encoding

For more information, check out our Bring Your Own Land blog post. Additionally, Mandiant experts from the FLARE team will present an in-depth view into UNC1945 on Thursday, Nov. 12. Register today to reserve your spot for this discussion, where the presenters from FLARE and Mandiant Managed Defense will also answer questions from the audience. Finally, for more intelligence on these types of threats, please register for Mandiant Advantage Free, a no-cost version of our threat intelligence platform.