

Security Report

Infection Monkey



Overview

⚠ Critical security issues were detected!

The first Infection Monkey Agent ran on `07/02/2023 13:28:43`. After `6 minutes and 2 seconds`, all Agents finished propagation attempts.

Infection Monkey started propagating from the following machines where it was manually installed:

- island-linux-250

Username available for brute-forcing:

- Administrator
- Guest
- DefaultAccount
- m0nk3y
- somenewuserfsczw
- user

Credentials available for brute-forcing:

- LM hash: aad*****
- NT hash: 94c*****
- Clear SSH private key: ---*****
- Clear Password: ^Ng*****

Configured exploitation methods:

- Hadoop/YARN Exploiter
- ZeroLogon Exploiter
- Log4Shell Exploiter
- SMB Exploiter
- PowerShell Remoting Exploiter
- WMI Exploiter
- MSSQL Exploiter
- SSH Exploiter

Configured IPs to scan:

- 10.2.2.9
- 10.2.3.45
- 10.2.3.47
- 10.2.3.48

- 10.2.1.10
- 10.2.0.11
- 10.2.2.15
- 10.2.2.25

Note: Infection Monkey was configured to avoid scanning the local network.

Machine-related Recommendations

- **tunneling-9 (10.2.1.9, 10.2.2.9)**

1. Change user passwords to a complex one-use password that is not shared with other computers on the network. Protect private keys with a pass phrase.

The machine is vulnerable to an SSH attack.
An Infection Monkey Agent authenticated over the SSH protocol.

Attempts a brute-force attack against SSH using known credentials, including SSH keys

2. Use micro-segmentation policies to disable communication other than the required.

Machines are not locked down at port level. Network tunnels were set up between the following.

- from tunneling-10 (10.2.0.10) to tunneling-9 (10.2.1.9)

- **smb-20 (10.2.2.25)**

1. Install Windows security updates.

The machine is vulnerable to a ZeroLogon exploit. This attack was possible because the latest security updates from Microsoft have not been applied to this machine. For more information about this vulnerability, see [this](#).

Exploits a privilege escalation vulnerability (CVE-2020-1472) in a Windows server domain controller (DC) by using the Netlogon Remote Protocol (MS-NRPC). This exploiter changes the password of a Windows server DC account, steals credentials, and then attempts to restore the original DC password. The victim DC will be unable to communicate with other DCs until the original password has been restored. If Infection Monkey fails to restore the password automatically, you'll have to do it manually. For more information, see the documentation.

- **mimikatz-15 (10.2.2.15)**

1. Change user passwords to a complex one-use password that is not shared with other computers on the network.

The machine is vulnerable to an SMB attack.

An Infection Monkey Agent authenticated over the SMB protocol.

Attempts a brute-force attack against SMB using known credentials

- **powershell-45 (10.2.3.47)**

1. Change user passwords to a complex one-use password that is not shared with other computers on the network.

The machine is vulnerable to an SMB attack.

An Infection Monkey Agent authenticated over the SMB protocol.

Attempts a brute-force attack against SMB using known credentials

- **powershell-45 (10.2.3.45, 10.2.4.45)**

1. Change user passwords to a complex one-use password that is not shared with other computers on the network.

The machine is vulnerable to an SMB attack.

An Infection Monkey Agent authenticated over the SMB protocol.

Attempts a brute-force attack against SMB using known credentials

- **tunneling-10 (10.2.0.10, 10.2.1.10)**

1. Change user passwords to a complex one-use password that is not shared with other computers on the network.
Protect private keys with a pass phrase.

The machine is vulnerable to an SSH attack.

An Infection Monkey Agent authenticated over the SSH protocol.

Attempts a brute-force attack against SSH using known credentials, including SSH keys

-
2. Use micro-segmentation policies to disable communication other than the required.

Machines are not locked down at port level. Network tunnels were set up between the following.

- from tunneling-10 (10.2.0.10) to tunneling-9 (10.2.1.9)

- 10.2.0.11 (10.2.0.11)

1. Change user passwords to a complex one-use password that is not shared with other computers on the network. Protect private keys with a pass phrase.

The machine is vulnerable to an SSH attack.

An Infection Monkey Agent authenticated over the SSH protocol.

Attempts a brute-force attack against SSH using known credentials, including SSH keys

The Network from Infection Monkey's Eyes

Infection Monkey discovered 7 machines and successfully breached 7 of them.

100% of scanned machines exploited

Infection Monkey discovered 0 open services on 7 machines:

Scanned Servers	
Machine	Services found
tunneling-9(10.2.1.9/32,10.2.2....	10.2.2.9:22 - unknown
smb-20(10.2.2.25/24)	10.2.2.25:135 - unknown 10.2.2.25:445 - unknown 10.2.2.25:3389 - unknown 10.2.2.25:5985 - unknown 10.2.2.25:5986 - unknown
mimikatz-15(10.2.2.15/24)	10.2.2.15:135 - unknown 10.2.2.15:445 - unknown 10.2.2.15:3389 - unknown 10.2.2.15:5985 - unknown 10.2.2.15:5986 - unknown
powershell-45(10.2.3.47/24)	10.2.3.47:135 - unknown 10.2.3.47:445 - unknown 10.2.3.47:3389 - unknown

	10.2.3.47:5985 - unknown
powershell-45(10.2.3.45/32,10....	10.2.3.45:135 - unknown 10.2.3.45:445 - unknown 10.2.3.45:3389 - unknown 10.2.3.45:5985 - unknown 10.2.3.45:5986 - unknown
tunneling-10(10.2.0.10/32,10.2....	10.2.1.10:22 - unknown
(10.2.0.11/32)	10.2.0.11:22 - unknown

Infection Monkey successfully breached 7 machines:


Breached Servers		
Machine	IP Addresses	Exploits
10.2.1.9	10.2.1.9 10.2.2.9	SSH Exploiter
10.2.2.25	10.2.2.25	Zerologon Exploiter SMB Exploiter
10.2.2.15	10.2.2.15	SMB Exploiter
10.2.3.47	10.2.3.47	SMB Exploiter
10.2.3.45	10.2.3.45 10.2.4.45	SMB Exploiter
10.2.0.10	10.2.0.10 10.2.1.10	SSH Exploiter
10.2.0.11	10.2.0.11	SSH Exploiter

Infection Monkey stole the following credentials:

Stolen Credentials	
Username	Type
Administrator	LM hash
Administrator	NT hash
Guest	LM hash
Guest	NT hash
krbtgt	LM hash

Previous

Page 1 of 6

5 rows 

Next

For questions, suggestions, or any other feedback, contact
support@infectionmonkey.com

