Security Report
Infection Monkey

Overview

Critical security issues were detected!

The first monkey run was started on 25/06/2020 11:23:15. After 8 minutes and 34 seconds, all monkeys finished propagation attempts.

The monkey started propagating from the following machines where it was manually installed:
- island-windows-251.c.guardicore-22050661.internal

The monkeys were run with the following configuration:

Usernames used for brute-forcing:
- m0nk3y

Passwords used for brute-forcing:
- Xk8******
- ^Ng******
- Ivr******
- 3Q=******
- `))******
- t67******

The Monkey uses the following exploit methods:
- SMB Exploiter
- WMI Exploiter
- MSSQL Exploiter
- SSH Exploiter
- ShellShock Exploiter
- SambaCry Exploiter
- Struts2 Exploiter
- Oracle WebLogic Exploiter
- Hadoop/Yarn Exploiter
- VSFTPD Backdoor Exploited

The Monkey scans the following IPs:
- 10.2.2.2
- 10.2.2.3
- 10.2.2.4
- 10.2.2.5
- 10.2.2.8
- 10.2.2.9
- 10.2.1.10
- 10.2.0.11
- 10.2.0.12
- 10.2.2.11
- 10.2.2.12
- 10.2.2.14
- 10.2.2.15
- 10.2.2.16
- 10.2.2.18
- 10.2.2.19
- 10.2.2.20
- 10.2.2.21
- 10.2.2.23
- 10.2.2.24

Note: Monkeys were configured to avoid scanning of the local network.

Security Findings

Immediate Threats

During this simulated attack the Monkey uncovered 2 threats:
- Machines are accessible using passwords supplied by the user during the Monkey's configuration.
- Hadoop/Yarn servers are vulnerable to remote code execution.

Potential Security Issues

The Monkey uncovered the following possible set of issues:

- Weak segmentation - Machines from different segments are able to communicate.
- Weak segmentation - Machines were able to communicate over unused ports.

Machine related recommendations

- ### UBUNTU-4UBUNTU2.8

  1. Run Hadoop in secure mode (add Kerberos authentication).

     The Hadoop server at Ubuntu-4ubuntu2.8 (10.2.2.2) is vulnerable to remote code execution attack.
     The attack was made possible due to default Hadoop/Yarn configuration being insecure.

- ### TUNNELING-10.C.GUARDICORE-22050661.INTERNAL

  1. Change m0nk3y 's password to a complex one-use password that is not shared with other computers on the network.

     The machine tunneling-10.c.guardicore-22050661.internal (10.2.1.10) is vulnerable to a SSH attack.
     The Monkey authenticated over the SSH protocol with user m0nk3y and its password.

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

     Machines are not locked down at port level. Network tunnel was set up from tunneling-10.c.guardicore-22050661.internal to tunneling-9.c.guardicore-22050661.internal.

- ### TUNNELING-9.C.GUARDICORE-22050661.INTERNAL

  1. Change m0nk3y 's password to a complex one-use password that is not shared with other computers on the network.

     The machine tunneling-9.c.guardicore-22050661.internal (10.2.2.9) is vulnerable to a SSH attack.
     The Monkey authenticated over the SSH protocol with user m0nk3y and its password.

  2. Segment your network and make sure there is no communication between machines from different segments.

     The network can probably be segmented. A monkey instance on tunneling-9.c.guardicore-22050661.internal in the networks could directly access the Monkey Island server in the networks 10.2.2.0/24.

- ### ISLAND-WINDOWS-251.C.GUARDICORE-22050661.INTERNAL

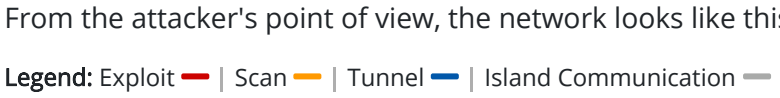
  1. Segment your network and make sure there is no communication between machines from different segments.

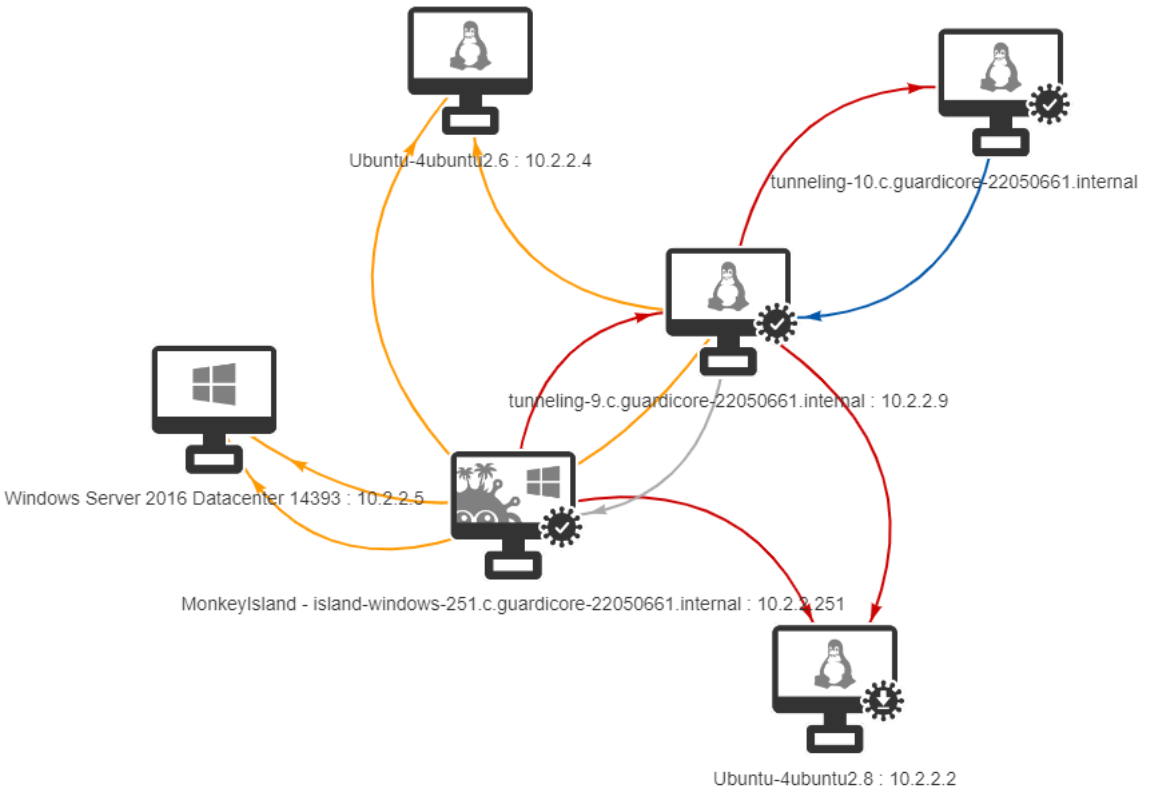
     The network can probably be segmented. A monkey instance on island-windows-251.c.guardicore-22050661.internal in the networks could directly access the Monkey Island server in the networks 10.2.2.0/24.

The Network from the Monkey's Eyes

The Monkey discovered 6 machines and successfully breached 3 of them.

From the attacker's point of view, the network looks like this:





The Monkey discovered 8 open services on 6 machines:

Scanned Servers			
Machine	IP Addresses	Accessible From	Services
Ubuntu-4ubuntu2.8	10.2.2.2	island-windows-251.c.guar tunneling-9.c.guardicore-2	tcp-22
Ubuntu-4ubuntu2.6	10.2.2.4	island-windows-251.c.guar tunneling-9.c.guardicore-2	tcp-9200 elastic-search-9200 tcp-22
Windows Server 2016 D...	10.2.2.5	island-windows-251.c.guar tunneling-9.c.guardicore-2	tcp-3389 elastic-search-9200 tcp-445
island-windows-251.c.g...	10.2.2.251		
tunneling-9.c.guardicor...	10.2.2.9 10.2.1.9	island-windows-251.c.guar tunneling-10.c.guardicore-	
tunneling-10.c.guardico...	10.2.1.10 10.2.0.10	tunneling-9.c.guardicore-2	tcp-22

The Monkey successfully breached 3 machines:

Breached Servers		
Machine	IP Addresses	Exploits
tunneling-9.c.guardicore-220506...	10.2.2.9 10.2.1.9	SSH Exploiter
tunneling-10.c.guardicore-22050...	10.2.1.10 10.2.0.10	SSH Exploiter
Ubuntu-4ubuntu2.8	10.2.2.2	Hadoop/Yarn Exploiter

The Monkey performed 5 post-breach actions on 3 machines:

Post breach actions
Machine
▸ island-windows-251.c.guardicore-22050661.internal (10.2.2.251)
▸ tunneling-9.c.guardicore-22050661.internal (10.2.2.9 10.2.1.9)
▸ tunneling-10.c.guardicore-22050661.internal (10.2.1.10 10.2.0.10)

Stolen Credentials		
Username	Type	Stolen From
vakaris_zilius	NTLM hash	island-windows-251.c.guardicore...
m0nk3y	Clear SSH private key	tunneling-9.c.guardicore-220506...
m0nk3y	Clear SSH private key	tunneling-10.c.guardicore-22050...

Powerful Users		
No rows found		
Username	Machines	Services

For questions, suggestions or any other feedback contact:
labs@guardicore.com

Guardicore