Cyber-Security Incident
Report

Prepared for: Ingenious Geeks

March 26, 2019

Incident Summary

This report summarizes the cyber security findings observed during the noted time period. Any other findings visible in the RocketCyber Console that are not represented in this report should be considered benign and will be purged from the dashboard. Of the 28 devices monitored, 7 devices reported detections between 03/22/19 1:53:37PM and 03/26/19 7:57:29AM across 9 RocketApps.

Malicious Detections

0

Suspicious Detections

32

Devices with Detections

7

RocketApps with Detections

9

Devices

Host	Customer	Detections	IP Address	
PROXXXX	UXXXX	1	192.168.1.68	Details
OP9XXXX	IXXXX	6	192.168.10.244	Details
KARXXXX	UXXXX	25	192.168.1.46	Details
SERXXXX	UXXXX	27	192.168.1.10	Details
TUSXXXX	BXXXX	59	192.168.1.3	Details
MAIXXXX	DXXXX	34	192.168.1.130	Details
MICXXXX	BXXXX	9	192.168.1.2	Details

Malicious File Detection

Monitoring

Monitors and detects suspicious and malicious files that are written to disk or executed.

Malicious Detections	Suspicious Detections
0	0

Suspicious Tools

Monitoring

This app detects programs that can negatively impact the security of the system and business network. Detected suspicious tools should be investigated and are categorized as hacking utilities, password crackers, or other tools used by attackers for malicious purposes.

Malicious Detections	Suspicious Detections
0	3

System Process Verifier

Monitoring

Detects and analyzes system processes for known suspicious or malicious behaviors based on various factors including disk image location, timestamp fingerprinting and Levenshtein distance calculations.

Malicious Detections	Suspicious Detections
0	0

Suspicious Event Monitor

Monitoring

The app monitors the Microsoft Windows Event Log for suspicious events. Detected events are security related activities such as failed logins, clearing security logs, unauthorized activity, etc.

Malicious Detections	Suspicious Detections
0	8

Advanced Breach Detection

Monitoring

This app identifies computers that are compromised where security defenses have been circumvented. Malicious activity reported by this app requires immediate investigation.

Malicious Detections	Suspicious Detections
0	0

Suspicious Network Services

Monitoring

This app detects suspicious network services running on an endpoint. While there are 65,535 available network services for legitimate use, suspicious detections are defined as well known ports and services that are leveraged for malicious intent.

Malicious Detections	Suspicious Detections
0	0

Crypto Mining Detection

Monitoring

Detects crypto mining activity form browser based crypto miners as well as common crypto mining client software.

Malicious Detections	Suspicious Detections
0	0

Basic Breach Detection

Monitoring

Provides Basic Breach detection capabilities by monitoring ASEP (Automated Software Extension Points) on Windows desktops and servers. Monitors for changes to these locations and evaluates the intended execution target.

Malicious Detections	Suspicious Detections
0	0

Cyber Terrorist Network Connections

Monitoring

This app detects network connections to various nation states that have been known to engage in cyberterrorist activities.

Malicious Detections	Suspicious Detections
0	21

PROXXXX 1 Detection

IP: 192.168.1.68 **OS:** Windows 7 Pro Service Pack 1 **MAC:** 6C:62:6D:EA:5E:3C

Incident #1

	Date/Time	App	Region	Country	Local port	Remote port	Local address	Remote address
⚠	03/25/19 3:23:17PM	Cyber Terrorist Network Connections		🇨🇳	62615	443	192.168.1.68	117.121.28.4

Notes: Web connection to China

Remediation: Uninstall any unnecessary browser plugins. Review browsing history Train user on safe browsing habits

OP9XX 6 Detections

IP: 192.168.10.244 **OS:** Windows 10 Pro **MAC:** F8:B1:56:D7:EB:D4

Incident #1

	Date/Time	App	Region	Country	Local port	Remote port	Local address	Remote address
⚠	03/25/19 4:11:39PM	Cyber Terrorist Network Connections		🇷🇺	59820	443	192.168.10.244	80.239.201.39
⚠	03/25/19 4:08:06PM	Cyber Terrorist Network Connections		🇷🇺	59820	443	192.168.10.244	80.239.201.90
⚠	03/25/19 4:08:05PM	Cyber Terrorist Network Connections		🇷🇺	65376	80	192.168.10.244	89.249.18.10
⚠	03/25/19 4:07:57PM	Cyber Terrorist Network Connections		🇷🇺	59820	443	192.168.10.244	217.69.133.211
⚠	03/25/19 4:07:48PM	Cyber Terrorist Network Connections		🇷🇺	59820	443	192.168.10.244	94.100.180.39

Notes: Various web connections to Russia

Remediation: Uninstall any unnecessary browser plugins. Verify default search engine.

KARXXX

25 Detections

IP: 192.168.1.46 **OS:** Windows 7 Pro Service Pack 1 **MAC:** F8:B1:56:BF:8F:D7

Incident #1

	Date/Time	App	Region	Country	Local port	Remote port	Local address	Remote address
⚠	03/25/19 6:53:59PM	Cyber Terrorist Network Connections	Novosibirsk	🇷🇺	59719	443	192.168.1.46	88.198.239.119
⚠	03/25/19 4:20:21PM	Cyber Terrorist Network Connections		🇷🇺	53	443	192.168.1.46	93.158.134.90
⚠	03/25/19 10:17:39AM	Cyber Terrorist Network Connections		🇨🇳	57991	443	192.168.1.46	117.121.28.4
⚠	03/22/19 1:53:37PM	Cyber Terrorist Network Connections	Beijing	🇨🇳	56266	443	192.168.1.46	54.222.238.19

Notes: Web connections to China and Russia

Remediation: Remove any browser plugins that aren't required. Verify browsing habits with user.

SERXXX

27 Detections

IP: 192.168.1.10 **OS:** Windows Server 2012-R2 Server Standard **MAC:** B0:83:FE:E1:5B:1C

Incident #1

	Date/Time	App
⚠	03/25/19 9:28:33PM	Suspicious Event Monitor
⚠	03/25/19 6:21:50PM	Suspicious Event Monitor
⚠	03/25/19 12:06:54PM	Suspicious Event Monitor
⚠	03/25/19 12:05:51PM	Suspicious Event Monitor
⚠	03/25/19 9:20:28AM	Suspicious Event Monitor
⚠	03/25/19 6:13:53AM	Suspicious Event Monitor
⚠	03/25/19 3:07:17AM	Suspicious Event Monitor
⚠	03/25/19 12:00:17AM	Suspicious Event Monitor

Notes: Several failed login attempts for Administrator account initiating from \\192.168.1.10.

Remediation: Verify that this is not an automated process running from this system that has an outdated cached password. Review the administrator account to determine if it has been locked out. Change the administrator account password.

TUSXXX 59 Detections

IP: 192.168.1.3 **OS:** Windows 7 Pro Service Pack 1 **MAC:** A4:1F:72:69:8F:D2

Incident #1

	Date/Time	App	Region	Country	Local port	Remote port	Local address	Remote address
⚠	03/26/19 1:52:31AM	Cyber Terrorist Network Connections	Beijing	🇨🇳	443	443	192.168.1.3	54.223.75.176
⚠	03/26/19 1:47:05AM	Cyber Terrorist Network Connections	Beijing	🇨🇳	32772	443	192.168.1.3	54.223.96.206
⚠	03/26/19 1:45:57AM	Cyber Terrorist Network Connections	Beijing	🇨🇳	32772	443	192.168.1.3	54.223.52.127
⚠	03/26/19 1:04:05AM	Cyber Terrorist Network Connections	Beijing	🇨🇳	57798	59709	192.168.1.3	203.208.43.95
⚠	03/25/19 11:54:54AM	Cyber Terrorist Network Connections	Beijing	🇨🇳	53135	443	192.168.1.3	203.208.40.56

Notes: Numerous connections to China.

Remediation: Inspect browsing history on this system to determine where and why these connections were made. Discuss safe browsing habits with user.

MAIXXXX **34 Detections**

IP: 192.168.1.130 **OS:** Windows 10 Pro **MAC:** 1C:1B:0D:0C:E7:63

Incident #1

	Date/Time	App
⚠	03/26/19 7:57:29AM	Suspicious Tools
⚠	03/26/19 7:57:28AM	Suspicious Tools
⚠	03/26/19 7:57:27AM	Suspicious Tools

Notes: Various tools found that should be considered suspicious

Remediation: Remove Bitcoin and Tor Browser. Remove Putty if not required for business purposes.

Incident #2

	Date/Time	App	Region	Country	Local port	Remote port	Local address	Remote address
⚠	03/25/19 6:08:49PM	Cyber Terrorist Network Connections		🇷🇺	53	443	192.168.1.130	213.180.204.90
⚠	03/25/19 6:01:49PM	Cyber Terrorist Network Connections		🇷🇺	58032	443	192.168.1.130	93.158.134.90

Notes: Web Connections to Russia

Remediation: Uninstall any unnecessary browser plugins Consult with user on safe browsing practices. Review browsing history in Chrome

MICXXXXX 9 Detections

IP: 192.168.1.2 **OS:** Windows 10 Pro **MAC:** B8:CA:3A:9F:DB:54

Incident #1

	Date/Time	App	Region	Country	Local port	Remote port	Local address	Remote address
⚠	03/25/19 5:17:31PM	Cyber Terrorist Network Connections		🇷🇺	63163	80	192.168.1.2	62.213.108.136
⚠	03/25/19 5:17:30PM	Cyber Terrorist Network Connections		🇷🇺	63163	80	192.168.1.2	62.213.108.142
⚠	03/25/19 3:23:27PM	Cyber Terrorist Network Connections	Saint Petersburg City	🇷🇺	54699	443	192.168.1.2	81.3.180.109
⚠	03/22/19 5:36:28PM	Cyber Terrorist Network Connections	Saint Petersburg City	🇷🇺	51296	443	192.168.1.2	81.3.180.109

Notes: Abby Fine Reader connections to Russia.

Remediation: AbbY Fine reader is an OCR product. Determine why it is connecting to Russia. If not required, uninstall this software product and find another compliant source.