Rocke'in the NetFlow

By Nathaniel Quist

Published: 2019-08-01 · Archived: 2026-04-05 22:28:55 UTC

Executive Summary

Unit 42 spent six months researching the China-based cybercrime group Rocke, which is the best-known threat actor engaged in cryptomining operations targeting the cloud. We released high-level results from our investigation of Rocke in our recent cloud threat report. This research report provides a deep dive into our investigation of Rocke, which concluded that the group is able to conduct operations with little interference and limited detection risk.

By analyzing NetFlow data from December 2018 to June 16, 2019, we found that 28.1% of the cloud environments we surveyed had at least one fully established network connection with at least one known Rocke command-and-control (C2) domain. Several of those organizations maintained near daily connections. Meanwhile, 20% of the organizations maintained hourly heartbeats consistent with Rocke tactics, techniques, and procedures (TTPs).

The group has also released a new tool called Godlua, which could function as an agent, allowing the group's actors to perform additional scripted operations, including denial of service (DoS) attacks, network proxying, and two shell capabilities. Unit 42 also discovered network traffic identification patterns within NetFlow traffic that provide unique insight into Rocke TTPs and how defenders can develop detection capabilities.

Intro to Rocke

The activities of Rocke, aka the Iron Group, SystemTen, Kerberods/Khugepageds, and even ex-Rocke, were originally reported in August 2018. Researchers have since blogged on its use of the Golang programming language and the new backdoor, Godlua. There is an operational blog mapping Rocke operations to the MITRE ATT&CK framework. Unit 42 has also published blogs on the group's Xbash ransomware tool and its cloud security evasion and cryptomining techniques.

Rocke was initially associated with ransomware campaigns through the use of its Linux-focused Xbash tool, a data-destruction malware similar in functionality to NotPetya. NotPetya used the EternalBlue exploit to propagate across a network. Xbash performed lateral movement by leveraging an organization's unpatched vulnerabilities and use of weak passwords, which potentially limited its overall effectiveness. When Rocke compromised an organization, it demanded that victims pay 0.2, 0.15, or 0.02 bitcoin (BTC) to restore lost data. However, Rocke was unable to restore any data since Xbash deleted database tables prior to demanding the ransom. At the time of Unit 42's reporting, Rocke's BTC wallet contained 0.964 BTC (equivalent to US$10,130 today) from just 48 unique transfers.

Rocke's Cryptomining Operation

Like Rocke's Xbash malware, the group's first cryptomining operations were written in Python and used Pastebin or GitHub as the code repository from which the first-stage payload was downloaded. As of March 12, 2019, Rocke actors began to also use Golang. The first-stage payload directed the victim system to connect to a hardcoded Rocke domain or IP address, which would trigger the download of the second-stage payload.

Unit 42 has observed a distinctive 12-step operation style, which appears to have remained consistent since Rocke was first reported:

- Actor uploads first payload to a third-party site (e.g., Pastebin, GitHub)
- Entices victim to navigate to Pastebin/GitHub (e.g., spear phishing)
- Exploits known vulnerability (e.g., Oracle WebLogic, Adobe ColdFusion, Apache Struts)
- Victim downloads backdoor (e.g., Shell Scripts, JavaScript Backdoor)
- Victim runs the first payload via Python or Golang script and connects to C2 server
- Downloads and executes second payload script, gaining administrative access to the system
- Establishes persistence via cron job commands
- Searchers for and kills previously installed cryptomining processes
- Adds "IPtables" rules to block future cryptomining processes
- Uninstalls agent-based cloud security tools (e.g., Tencent Cloud, Alibaba Cloud)
- Downloads and installs Monero mining software
- Rootkits XMRig mining processes from Linux "ps" using "libprocesshider"

Rocke Infrastructure

As of the time of this writing, eight domains have been tied to Rocke C2 operations through hardcoded IP addresses, URL addresses, or domain registration connections (e.g., WHOIS registrant email address). The following chart lays out how the domains fit into the Rocke group infrastructure (see Table 1).

Domain	Rocke Connection	Connection Value	Resolved IP(s)
sowcar[.]com	Hardcode IOC	4592248@gmail[.]com	23.234.4[.]151 23.234.4[.]153 27.221.28[.]231 27.221.54[.]252 36.103.236[.]221 36.103.247[.]121 36.248.26[.]205 42.202.141[.]230 42.236.125[.]84

			42.56.76[.]104 43.242.166[.]88 59.83.204[.]14 60.167.222[.]122 61.140.13[.]251 104.31.68[.]79 104.31.69[.]79 113.142.51[.]219 113.200.16[.]234 116.211.184[.]212 118.213.118[.]94 118.25.145[.]24 122.246.6[.]183 125.74.45[.]101 150.138.184[.]119 182.118.11[.]126 182.118.11[.]193 182.247.250[.]251 182.247.254[.]83 183.224.33[.]79 211.91.160[.]159 211.91.160[.]238 218.75.176[.]126 219.147.231[.]79 221.204.60[.]69
thyrsi[.]com	WHOIS Registration	4592248@gmail[.]com	23.234.4[.]151

			23.234.4[.]153 103.52.216[.]35 104.27.138[.]223 104.27.139[.]223 205.185.122[.]229 209.141.41[.]204
w2wz[.]cn	WHOIS Registration	4592248@gmail[.]com	36.103.236[.]221 36.103.247[.]121 42.202.141[.]230 58.215.145[.]137 58.216.107[.]77 58.218.208[.]13 60.167.222[.]122 61.140.13[.]251 113.142.51[.]219 113.96.98[.]113 116.211.184[.]212 118.213.118[.]94 118.25.145[.]241 121.207.229[.]203 122.246.20[.]201 125.74.45[.]101 140.249.61[.]134 150.138.184[.]119 182.118.11[.]193 182.247.250[.]251

			218.75.176[.]126 219.147.231[.]79 222.186.49[.]224
baocangwh[.]cn	WHOIS Registration	4592248@qq[.]com	103.52.216[.]35 104.18.38[.]253 104.18.39[.]253 104.31.92[.]26 104.31.93[.]26 119.28.48[.]240 205.185.122[.]229
z9ls[.]com	WHOIS Registration	4592248@qq[.]com	103.52.216[.]35 104.27.134[.]168 104.27.135[.]168 104.31.80[.]164 104.31.81[.]164 172.64.104[.]10 172.64.105[.]10 205.185.122[.]229
gwjyhs[.]com	Hardcoded Domain	gwjyhs[.]com	103.52.216[.]35 104.27.138[.]191 104.27.139[.]191 205.185.122[.]229
heheda[.]tk	Hardcode IP or Domain	104.238.151.101 c.heheda[.]tk d.heheda[.]tk	104.18.58[.]79 104.18.59[.]79 104.238.151[.]101

		dd.heheda[.]tk	195.20.40[.]95 198.204.231[.]250
cloudappconfig[.]com	Hardcode IP or Domain	104.238.151.101 c.cloudappconfig[.]com img0.cloudappconfig[.]com Img1.cloudappconfig[.]com img2.cloudappconfig[.]com	43.224.225[.]220 67.21.64[.]34 104.238.151[.]101 198.204.231[.]250
systemten[.]org	Hardcoded Domain	systemten[.]org	104.248.53[.]213 104.31.92[.]233 104.31.93[.]233 134.209.104[.]20 165.22.156[.]147 185.193.125[.]146

Table 1. Known Rocke domains

Rocke New Attack Vector

The TTPs listed in the previous section do not take into account a potential third stage to Rocke operations. Prior to the report An Analysis of Godlua Backdoor, Rocke malware appeared to perform a single operational function upon compromised cloud systems. The Godlua report cited malware samples that contained similar TTPs to those of Rocke. Upon further research, Unit 42 identified that not only do the TTPs match, but there are hardcoded domains, URLs, and an IP address that overlap with previously reported Rocke malware hardcoded values. This connection was made possible through the findings of an incident investigation posting on the r/LinuxMalware subreddit and the upload of the findings, including malware sample metadata, to GitHub. The author of the Reddit post operates the nonprofit organization MalwareMustDie, a white hat organization devoted to the reduction of internet malware. Unit 42 researchers analyzed four of the binaries listed in the Reddit thread and confirmed the hardcoded Rocke domain systemten[.]org contained within the samples, which was stated in the Reddit thread. The samples also contained hardcoded links to the Pastebin URLs that overlap with known Rocke reporting:

- hxxps://pastebin[.]com/raw/HWBVXK6H
- hxxps://pastebin[.]com/raw/60T3uCcb
- hxxps://pastebin[.]com/raw/rPB8eDpu

- hxxps://pastebin[.]com/raw/wR3ETdbi
- hxxps://pastebin[.]com/raw/Va86JYqw
- hxxps://pastebin[.]com/raw/Va86JYqw

As seen within the Godlua blog, the IP address 104.238.151[.]101 and the URLs d.heheda[.]tk, c.heheda[.]tk, and dd.heheda[.]tk were found to be hardcoded within the report's findings. The incident response thread posted to Reddit pertaining to the Rocke group also found that C2 connections were being sent to the three heheda[.]tk domains, which resolved to the IP address 104.238.151[.]101, also cited in the Godlua report. Additionally, the samples contained hardcoded values for the known Rocke domains of sowcar[.]com, z9ls[.]com, baocangwh[.]cn, gwjyhs[.]com, and w2wz[.]cn. See Figure 1 for how the identified indicators of compromise (IoCs) connect known Rocke domains with the IoCs pulled from the Godlua and Reddit thread IoC reporting.

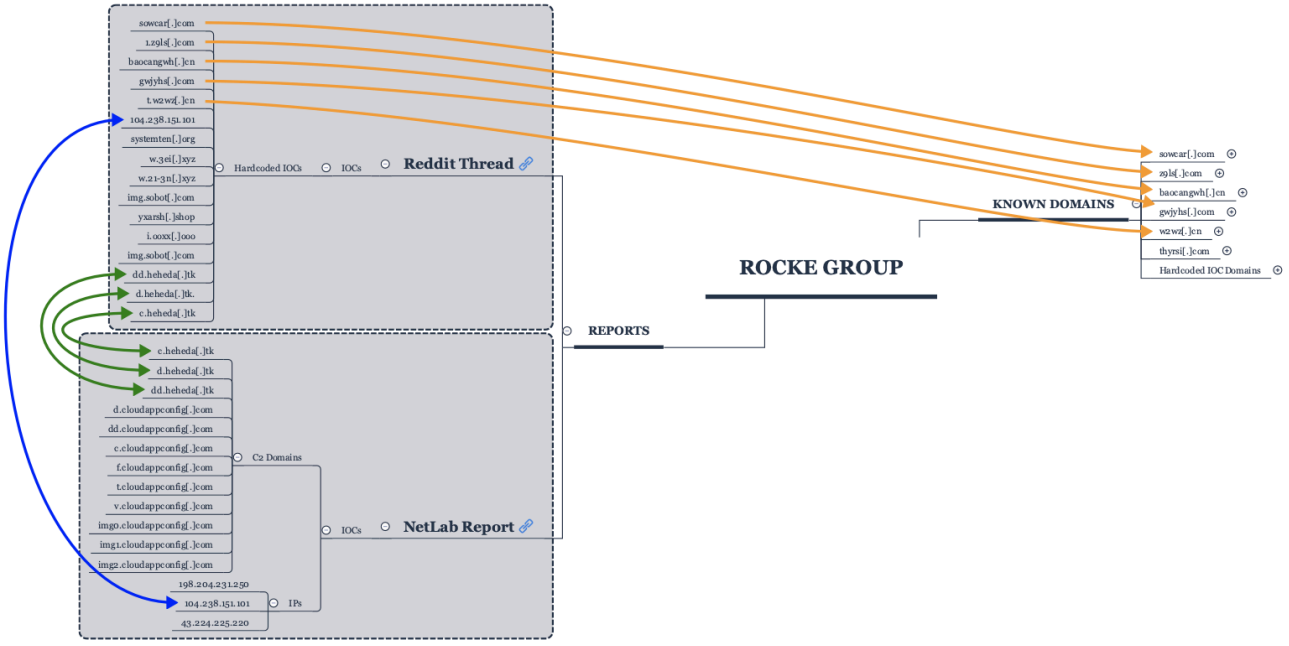

Figure 1. Rocke domain connections to Godlua and Reddit thread reporting

What makes the Godlua samples intriguing is the evidence that Rocke has added DoS operations to the group's toolkit. The report delivers evidence that Rocke has added a third-stage malware component that performs a third C2 request to either c.heheda[.]tk or c.cloudappconfig[.]com and thereby downloads a LUA script called Godlua. The malware appears to provide a modular functionality to Rocke's operational playbook. In addition to the DoS feature, the malware introduces the following new features:

- HANDSHAKE
- HEARTBEAT
- LUA
- SHELL
- UPGRADE
- QUIT
- SHELL2

- PROXY

The Godlua report also provided evidence that Rocke has added LUA switch functionality. The report states actors performed a DoS attack against the domain www.liuxiaobei[.]com. At the time of this writing, this domain does not resolve to any known system. It is currently unknown what functionality the other features of the Stage 3 malware accomplish. However, with options like “Shell,” “Shell2,” “Upgrade,” and “Proxy,” it is possible this malware is the beginning of a modular system agent that allows Rocke actors additional flexibility to perform cyber operations outside of cryptomining or data destruction.

Finding Rocke in the NetFlow

As of the time of this writing, Unit 42 researchers found 28.1% of cloud environments surveyed had at least one active communication session with known Rocke C2 domains. These connections occurred almost daily in some organizations from at least December 2018 until the time of this writing. Identification was made possible via the capture of NetFlow communications at the organization/cloud edge.

Unit 42 researchers discovered Rocke communications by analyzing Rocke’s TTP patterns, resolving the known Rocke domains to IP addresses used during the specified timeframe, and querying network traffic against these resolved IP address as well as the hardcoded IP address linked to Rocke, 104.238.151[.]101.

Hardcoded IP addresses provide strong connections to known malicious network traffic originating from an organization’s network. At the time of this writing, 104.238.151[.]101 is known to have resolved to the following URLs since January 1, 2019:

- c.cloudappconfig[.]com
- d.cloudappconfig[.]com
- f.cloudappconfig[.]com
- img0.cloudappconfig[.]com
- img2.cloudappconfig[.]com
- v.cloudappconfig[.]com
- c.heheda[.]tk
- d.heheda[.]tk
- dd.heheda[.]tk

These URLs are consistent with those reported in both the Godlua and Reddit reporting, signifying that any connection to this IP address should be considered malicious. Unit 42 researchers identified 411 unique connections from four monitored organizations that made eight or more fully established network connections to the IP address 104.238.151[.]101. These connections only persisted with each organization for a short period of time. The longest delta between first-seen connection and last-seen connection was five days for Organization 1. The shortest delta resulting in a single connection was one hour for Organization 4 (see Table 2).

Organization	Destination IP	Total Connections	Earliest Time	Latest Time
1	104.238.151[.]101	76	4/12/19 3:00 AM	4/17/19 8:00 AM

2	104.238.151[.]101	160	4/13/19 7:00 AM	4/15/19 3:00 PM
3	104.238.151[.]101	167	4/13/19 7:00 AM	4/16/19 10:00 AM
4	104.238.151[.]101	8	5/10/19 9:00 PM	5/10/19 9:00 PM

Table 2. Organization connections to hardcoded IP 104.238.151[.]101

Extrapolating from 104.238.151[.]101, these four organizations also connected to other known Rocke domains. Organization 1 connected to three Rocke domains between April 12 and May 31, 2019, with 290 unique connections. Organization 4 connected to seven domains between March 20 and May 15, 2019, with 8,231 unique connections. As is evident in Table 3, the four organizations connect to one or more of the seven known Rocke domains during the same timeframe as the organization's connections to the hardcoded IP address 104.238.151[.]101. This strongly favors the connection between the domains heheda[.]tk and cloudappcloudconfig[.]com as Rocke domains and the usage of Rocke's third-stage malware being available during this same time period.

Organization	**Destination Domain**	**Destination IP**	**Total Connections**	**Earliest Time**	**Latest Time**
1	**Heheda[.]tk | cloudappconfig[.]com**	**104.238.151[.]101**	76	4/12/19 3:00 AM	4/17/19 8:00 AM
	sowcar[.]com	125.74.45[.]101	4	4/12/19 2:00 PM	4/12/19 2:00 PM
		27.221.54[.]252	2	4/13/19 4:00 AM	4/13/19 4:00 AM
	systemten[.]org	104.248.53[.]213	202	4/10/19 12:00 PM	5/31/19 6:00 PM
	w2wz[.]cn	113.96.98[.]113	2	4/12/19 2:00 PM	4/12/19 2:00 PM
		125.74.45[.]101	4	4/12/19 2:00 PM	4/12/19 2:00 PM
1 Total			***290***		
2	baocanwh[.]cn	104.31.92[.]26	8	4/25/19 3:00 AM	4/25/19 3:00 AM
	heheda[.]tk	104.18.58[.]79	26	4/14/19 6:00 AM	4/15/19 3:00 PM

	heheda[.]tk	104.18.59[.]79	22	4/14/19 6:00 AM	4/15/19 2:00 PM
	Heheda[.]tk | **cloudappconfig[.]com**	**104.238.151[.]101**	160	4/13/19 7:00 AM	4/15/19 2:00 PM
	sowcar[.]com	104.31.68[.]79	77	3/20/19 11:00 PM	4/3/19 4:00 AM
		104.31.69[.]79	70	3/20/19 7:00 AM	4/10/19 9:00 AM
		125.74.45[.]101	6	4/12/19 1:00 PM	4/12/19 2:00 PM
		27.221.54[.]252	6	4/13/19 4:00 AM	4/13/19 4:00 AM
	systemten[.]org	104.248.53[.]213	92	4/11/19 5:00 PM	4/15/19 3:00 PM
	w2wz[.]cn	113.96.98[.]113	9	4/12/19 2:00 PM	4/12/19 6:00 PM
		122.246.20[.]201	8	4/22/19 7:00 AM	4/22/19 8:00 AM
		125.74.45[.]101	6	4/12/19 1:00 PM	4/12/19 2:00 PM
	z9ls[.]com	104.31.80[.]164	2	4/14/19 11:00 AM	4/14/19 11:00 AM
		104.31.81[.]164	4	4/15/19 3:00 AM	4/15/19 1:00 PM
2 Total			***496***		
3	heheda[.]tk	104.18.58[.]79	14	4/14/19 11:00 AM	4/16/19 10:00 AM
	heheda[.]tk	104.18.59[.]79	14	4/14/19 11:00 AM	4/16/19 10:00 AM

	Heheda[.]tk | **cloudappconfig[.]com**	**104.238.151[.]101**	167	4/13/19 7:00 AM	4/16/19 10:00 AM
	sowcar[.]com	104.31.68[.]79	2	4/10/19 9:00 AM	4/10/19 9:00 AM
	systemten[.]org	104.248.53[.]213	214	4/10/19 9:00 AM	4/19/19 9:00 AM
	z9ls[.]com	104.31.80[.]164	106	4/14/19 9:00 AM	4/18/19 3:00 AM
		104.31.81[.]164	108	4/14/19 9:00 AM	4/18/19 3:00 AM
3 Total			***625***		
4	baocanwh[.]cn	104.18.38[.]253	136	4/26/19 9:00 PM	4/27/19 3:00 PM
		104.18.39[.]253	152	4/26/19 10:00 PM	4/28/19 3:00 AM
		104.31.92[.]26	184	4/22/19 9:00 AM	4/26/19 6:00 PM
		104.31.93[.]26	170	4/22/19 9:00 AM	4/26/19 6:00 PM
		119.28.48[.]240	176	4/27/19 1:00 PM	4/28/19 10:00 AM
	gwjyhs[.]com	104.27.138[.]191	256	4/28/19 11:00 AM	5/9/19 10:00 AM
		104.27.139[.]191	256	4/28/19 10:00 AM	5/12/19 5:00 PM
	Heheda[.]tk | **cloudappconfig[.]com**	**104.238.151[.]101**	8	5/10/19 9:00 PM	5/10/19 9:00 PM
	sowcar[.]com	104.31.68[.]79	437	3/20/19 7:00 AM	4/10/19 2:00 AM

		104.31.69[.]79	441	3/20/19 2:00 PM	4/10/19 2:00 AM
		27.221.54[.]252	8	4/13/19 4:00 AM	4/13/19 4:00 AM
	systemten[.]org	104.31.93[.]233	4	4/5/19 2:00 AM	4/5/19 3:00 AM
		104.31.92[.]233	4	4/5/19 2:00 AM	4/5/19 3:00 AM
		104.248.53[.]213	4761	4/3/19 4:00 AM	5/15/19 1:00 AM
	thyrsi[.]com	103.52.216[.]35	178	4/27/19 8:00 AM	5/10/19 1:00 PM
	w2wz[.]cn	118.25.145[.]241	12	4/13/19 5:00 AM	4/13/19 9:00 AM
	z9ls[.]com	104.31.80[.]164	522	4/13/19 9:00 AM	4/21/19 2:00 PM
		104.31.81[.]164	526	4/13/19 6:00 AM	4/21/19 2:00 PM
4 Total			***8231***		
Grand Total			**9642**		

Table 3. Comparison of all Rocke domain connections with IP 104.238.151[.]101

Unit 42 researchers extrapolated the investigation another level and identified all visible connections from all monitored organizations to all known Rocke domains. The researchers found that 28.1% of cloud environments contained at least one fully established network connection with a known Rocke domain. The earliest witnessed connection took place on December 4, 2018, and continued through at least June 10, 2019, with 146 unique connections to the domains sowcar[.]com and w2wz[.]cn during that time frame.

Rocke's Network Traffic Pattern

Finally, Unit 42 researchers attempted to identify if the initial payload downloaded from Pastebin could be identified with the NetFlow data. Researchers found that a total of 50 organizations made network connections to Pastebin. Of these 50 organizations, eight were found to have made network connections to Pastebin within the same hour as connections to Rocke domains. Since NetFlow traffic only allows for a granularity capability of one hour, and given the lack of full packet capture to confirm the nature of the network connection, it is impossible to

positively identify precisely what time an organization was compromised. However, these occurrences point to key timeframes where full packet captures, if available, should be investigated further.

A distinct pattern emerges when viewing how Rocke network traffic appears within NetFlow data (see Figure 2). First, a connection is established with Pastebin, followed by a connection to a Rocke domain. As you can see from the image, the pattern repeats on an hourly basis, which is another indicator of beaconing capabilities and of the presence of the Stage 3 Rocke payload, which is already installed on the cloud system. Additionally, Figure 2 displays the unique occurrence of the source system connecting to Pastebin, then connecting to the known Rocke domains, z9ls[.]com, and systemten[.]org, connecting to the hardcoded IP address 104.238.151[.]101 in the same time frame. This pattern is indicative of a beaconing, or a heartbeat style of activity, which is a capability within the third-stage malware's feature set.

Domain	Timestamp	Source IP	Destination IP
systemten	4/16/19 7:00 AM	83. .63	104.248.53.213
pastebin	4/16/19 8:00 AM	83. .63	104.20.209.21
pastebin	4/16/19 8:00 AM	83. .63	104.20.209.21
pastebin	4/16/19 8:00 AM	83. .63	104.20.208.21
pastebin	4/16/19 8:00 AM	83. .63	104.20.208.21
z9ls	4/16/19 8:00 AM	83. .63	104.31.81.164
z9ls	4/16/19 8:00 AM	83. .63	104.31.81.164
z9ls	4/16/19 8:00 AM	83. .63	104.31.80.164
z9ls	4/16/19 8:00 AM	83. .63	104.31.80.164
systemten	4/16/19 8:00 AM	83. .63	104.248.53.213
systemten	4/16/19 8:00 AM	83. .63	104.248.53.213
pastebin	4/16/19 9:00 AM	83. .63	104.20.208.21
pastebin	4/16/19 9:00 AM	83. .63	104.20.208.21
pastebin	4/16/19 9:00 AM	83. .63	104.20.209.21
pastebin	4/16/19 9:00 AM	83. .63	104.20.209.21
z9ls	4/16/19 9:00 AM	83. .63	104.31.80.164
z9ls	4/16/19 9:00 AM	83. .63	104.31.80.164
z9ls	4/16/19 9:00 AM	83. .63	104.31.81.164
z9ls	4/16/19 9:00 AM	83. .63	104.31.81.164
systemten	4/16/19 9:00 AM	83. .63	104.248.53.213
systemten	4/16/19 9:00 AM	83. .63	104.248.53.213
pastebin	4/16/19 10:00 AM	83. .63	104.20.209.21
pastebin	4/16/19 10:00 AM	83. .63	104.20.209.21
pastebin	4/16/19 10:00 AM	83. .63	104.20.208.21
pastebin	4/16/19 10:00 AM	83. .63	104.20.208.21
z9ls	4/16/19 10:00 AM	83. .63	104.31.81.164
z9ls	4/16/19 10:00 AM	83. .63	104.31.81.164
heheda	4/16/19 10:00 AM	83. .63	104.238.151.101
heheda	4/16/19 10:00 AM	83. .63	104.238.151.101
heheda	4/16/19 10:00 AM	83. .63	104.238.151.101
heheda	4/16/19 10:00 AM	83. .63	104.238.151.101
systemten	4/16/19 10:00 AM	83. .63	104.248.53.213
systemten	4/16/19 10:00 AM	83. .63	104.248.53.213

Figure 2. Unique Rocke NetFlow pattern

Mitigation Strategies

To mitigate Rocke activities within a cloud environment, the following actions are recommended:

- Update all cloud system templates with the latest patches and version updates.
- Cycle all cloud systems to use the latest patched and updated cloud template.
- Purchase and configure a cloud monitoring product that includes checks on compliance, network traffic, and user behavior.
- Review cloud network configurations, security policies, and groups to ensure they meet current compliance requirements.
- Use a cloud container vulnerability scanner.
- Update all threat intelligence feeds providing domain or IP denylisting indicators.
- Purchase or subscribe to Palo Alto Networks MineMeld threat feed, or use Palo Alto Networks Next-Generation Firewalls, as these options are configured to block known Rocke domains and IP connections.
- Investigate cloud network traffic for connections to known malicious domains or IPs.
- Investigate cloud network traffic for beacon-style egress traffic in your organization's cloud environment.

Conclusion

Rocke, which primarily targets public cloud infrastructure for criminal gain, continues to evolve its tools and take advantage of poorly configured cloud infrastructures using vulnerabilities released in 2016 and 2017. The group can gain administrative access to cloud systems using malware that is able to remain hidden from basic investigations. Compromised systems then perform predictable and detectable network actions to known Rocke hardcoded IP addresses or Rocke-owned domains.

Palo Alto Networks customers are protected as follows:

- The C2 domains listed in this blog are identified as malicious by our PAN-DB URL Filtering.
- All illegitimate tools uploaded to the webshells are identified as malicious by WildFire and Traps.
- ELF and PE format malware signatures have been released via antivirus.
- All C2 domains have been covered by PAN-DB URL Filtering.

AutoFocus customers can investigate this activity with the following tags:

- IronCybercrimeGroup
- Xbash
- Kerberods
- Godlua

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Indicators of Compromise

Domains

sowcar[.]com

thyrsi[.]com

w2wz[.]cn

baocangwh[.]cn

z9ls[.]com

gwjyhs[.]com

heheda[.]tk

cloudappconfig[.]com

systemten[.]org

IPs

43.224.225[.]220

67.21.64[.]34

103.52.216[.]35

104.248.53[.]213

104.238.151[.]101

198.204.231[.]250

205.185.122[.]229

Hashes

1608899ff3bd9983df375fd836464500f160f6305fcc35cfb64abbe94643c962

28f92f36883b69e281882f19fec1d89190e913a4e301bfc5d80242b74fcba6fe

a84283095e0c400c3c4fe61283eca6c13dd0a6157a57adf95ae1dcec491ec519

6797018a6f29ce3d447bd3503372f78f9513d4648e5cd3ab5ab194a50c72b9c4
