SEQURETEK
SIMPLIFY SECURITY

Cyber Threat Advisory - SQTK/ADV/2024/0036

Cuttlefish: The Lurking Malware Hijacking Your Network - IoCs

Payload Server and corresponding file hashes:

Payload Server URL	File Hash
hxxp://209.141.49[.]178/dajfdsfadsfa/arm	10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62702f18d919e89
hxxp://209.141.49[.]178/dajfdsfadsfa/i386	94812d391160e4fce821701b944cfd8f5fd9454b3cbb8e8974d1dc259310e500
hxxp://209.141.49[.]178/dajfdsfadsfa/i386_i686	4aa23fbdc27d317c6e54481b6d884b962adf6e691a4731c859ddaf9af09822c6
hxxp://209.141.49[.]178/dajfdsfadsfa/i386_x64	1168e97ccf61600536e93e9c371ee7671bae4198d4bf566550328b241ec52e89
hxxp://209.141.49[.]178/dajfdsfadsfa/misp32	70693211cd0b14a7463b39b2fa801ce1fdefc85c7f3e003772d1b4deeb78efde
hxxp://209.141.49[.]178/dajfdsfadsfa/misp64	2f0911fb892d448910c36a37c9fbdec8c73ccfecc274854b1fa053fb1cc2369b

Malicious Payload Files:

File Path	File Hash
/r/s.sh	07df37d8168e911b189bbe0912b4842fa1fe48d5264e99738ad3247f9c818478
/r/arm_sniff	6295d5cb21c441066d2da81a76440bcac9bd5a7830fc9faea9668bd0b2015046
/r/i386_i686_sniff	eb7a7ab952080f66c82fe8350da131ce0d7766f203bd4d97b0798b4f59283a27
/r/i386_sniff	99d5cf32f8198e99c530be4f5e05487e280bacdb8ef26aaf38dc20e301aad75f
/r/i386_x64_sniff	3d9ee05c0841ad65547c0cc8516d092cff48dad5e7bbf97c99ddd44ee94a24bc
/r/mips32_sniff	2ed174523bd80a93b7d09940d375f9c0d71e1ce8ecffb2320e02a78f4b601408

Primary Command and Control Servers:

Server URL
hxxps://205.185.122[.]121/rules
hxxps://205.185.122[.]121/upload
hxxps://205.185.122[.]121/rulesinit
hxxps://198.98.56[.]93:443/rules
hxxps://198.98.56[.]93:443/rulesinit
hxxps://198.98.56[.]93:443/upload hxxps://107.189.28[.]251:443/rules hxxps://kkthreas[.]com/upload
hxxps://kkthreas[.]com
hxxps://pp.kkthreas[.]com

On Disk Files

File Path
/tmp/.timezone
/tmp/co.tmp.tar.gz
/tmp/config js
/tmp/log.txt
/tmp/n2nconfigjs
/tmp/thconfigjs
/tmp/.Pg88s51gQG4tFyImFsT9qy6ZM5TeTF8.so
/tmp/.putin

TCP/UDP port numbers:

Protocol	Port Number	Service
TCP	21	FTP
TCP	22	SSH
TCP	23	Telnet
TCP	25	SMTP
TCP	53	DNS
UDP TCP	53 69	DNS TFTP

Protocol	Port Number	Service
TCP	80	HTTP
TCP	81	HTTP Alternate
TCP	82	HTTP Alternate
TCP	83	HTTP Alternate
TCP	88	Kerberos
TCP	110	POP3
TCP	135	MSRPC
TCP	139	NetBIOS Session Service
TCP	143	IMAP
TCP	164	CMIP/TCP
TCP	389	LDAP
TCP	443	HTTPS
TCP	444	SNPP
TCP	445	Microsoft-DS (Active Directory)
TCP	554	RTSP
TCP	888	CD Database Protocol (CDDBP)
TCP	992	Telnet over SSL/TLS
TCP	993	IMAPS (IMAP over SSL/TLS)
TCP	995	POP3S (POP3 over SSL/TLS)
TCP	1024	Reserved
TCP	1080	SOCKS Proxy
TCP	1194	OpenVPN
TCP	1433	Microsoft SQL Server
TCP	1443	Microsoft SQL Server
TCP	1521	Oracle Database
TCP	1701	L2TP
TCP	1723	PPTP
TCP	1935	Adobe Flash
TCP	2000	Cisco SCCP
TCP	2103	Zephyr Notification Service
TCP	2222	DirectAdmin
TCP	2323	Telnet
TCP	2375	Docker API
TCP	2600	Zebra
TCP	2601	Zebra

Protocol	Port Number	Service
TCP	3128	Squid Proxy
TCP	3306	MySQL
TCP	3333	Network Lens
TCP	3389	Remote Desktop Protocol (RDP)
TCP	3443	Google Cloud Printer Secure
TCP	4343	Unicenter NSM Secure
TCP	4430	Red Hat Satellite
TCP	4433	Secure Domain Toolkit

Keywords Searched for in URLs

Keywords Searched		
username=	amazonaws=	authsecret=
user_name=	ansible_vault_password=	aws_access=
username	aos_key=	aws_access_key_id=
account=	api_key=	aws_bucket=
passwd	api_key_secret=	aws_key=
password	api_key_sid=	aws_secret=
<passwd>	api_secret=	aws_secret_key=
<pass_word>	api.googlemaps AIza=	aws_token=
<userName>	apidocs=	AWSSecretKey=
<password>	apikey=	b2_app_key=
passwd=	apiSecret=	bashrc password=
password=	app_debug=	bintray_apikey=
pass_word=	app_id=	bintray_gpg_password=
Authorization:	app_key=	bintray_key=
access_key=	app_log_level=	bintraykey=
access_token=	app_secret=	bluemix_api_key=
admin_pass=	appkey=	bluemix_pass=
admin_user=	appkeysecret=	browserstack_access_key=
algolia_admin_key=	application_key=	bucket_password=
algolia_api_key=	appsecret=	bucketeer_aws_access_key_id=
alias_pass=	appspot=	bucketeer_aws_secret_access_key=
alicloud_access_key=	auth_token=	built_branch_deploy_key=

amazon_secret_access_key=	authorizationToken=	bx_password=
cache_s3_secret_key=	cloud_watch_aws_access_key=	cache_driver=
cattle_access_key=	cloudant_password=	connectionstring=
cattle_secret_key=	cloudflare_api_key=	consumer_key=
certificate_password=	cloudflare_auth_key=	consumer_secret=
ci_deploy_password=	cloudinary_api_secret=	credentials=
client_secret=	cloudinary_name=	cypress_record_key=
client_zpk_secret_key=	codecov_token=	database_password=
clojars_password=	config=	database_schema_test=
cloud_api_key=	conn.login=	datadog_api_key=
db_server=	dot-files=	datadog_app_key=
db_username=	dotfiles=	db_password=
dbpasswd=	droplet_travis_password=	
dbpassword=	dynamoaccesskeyid=	
dbuser=	dynamosecretaccesskey=	
deploy_password=	elastica_host=	
digitalocean_ssh_key_body=	elastica_port=	
digitalocean_ssh_key_ids=	elasticsearch_password=	
docker_hub_password=	encryption_key=	
docker_key=	encryption_password=	
docker_pass=	env.heroku_api_key=	
docker_passwd=	env.sonatype_password=	
docker_password=	eureka.awssecretkey=	
dockerhub_password=	dockerhubpassword=	

(Note: *The TCP ports and keywords provided herein are solely for informational purposes and are not necessarily employed for malicious activities associated exclusively by the malware. It is crucial to ensure continuous monitoring of their usage. Please refrain from directly blocking them; instead, keep them under observation to maintain network security.)*

MITRE ATT&CK TACTICS AND TECHNIQUES

Technique Title	ID	Use
Reconnaissance		
Network Sniffing (T1040)	T1040	Cuttlefish eavesdrops on network traffic using libpcap and eBPF filters to gather information about the network and potential targets.

Technique Title	ID	Use
Resource Development		
Remote System Discovery (T1018)	T1018	Cuttlefish retrieves configuration updates and policies from the C2 server to enhance its capabilities and adapt to the target environment.
Initial Access		
Exploit Public-Facing Application (T1190)	T1190	Initial access vector remains unidentified, but Cuttlefish is deployed using a bash script that likely exploits vulnerabilities in public-facing services or devices.
Execution		
Command and Scripting Interpreter (T1059)	T1059	Cuttlefish employs a bash script to download and execute the trojan on compromised devices, ensuring its presence in memory and avoiding detection.
Persistence		
Boot or Logon Autostart Execution (T1547)	T1547.001	Cuttlefish ensures its persistence by remaining in memory and evading detection mechanisms. It hides its presence by deleting the file from the file system after execution.
Defense Evasion		
File Deletion (T1107)	T1107	Cuttlefish deletes the trojan file from the file system after execution, making it difficult to detect and remove.
Credential Access		
Credentials from Web Browsers (T1555.003)	T1555.003	Cuttlefish targets web requests passing through the router's LAN to steal authentication materials, potentially compromising credentials associated with cloud-based services.
Discovery		
Network Service Scanning (T1046)	T1046	Cuttlefish scans network traffic across selected interfaces to identify potential targets and gather information about the network.
Collection		
Data Staged (T1074)	T1074	Cuttlefish compresses and uploads log files containing stolen data to the C2 server, facilitating data collection.
Command and Control		

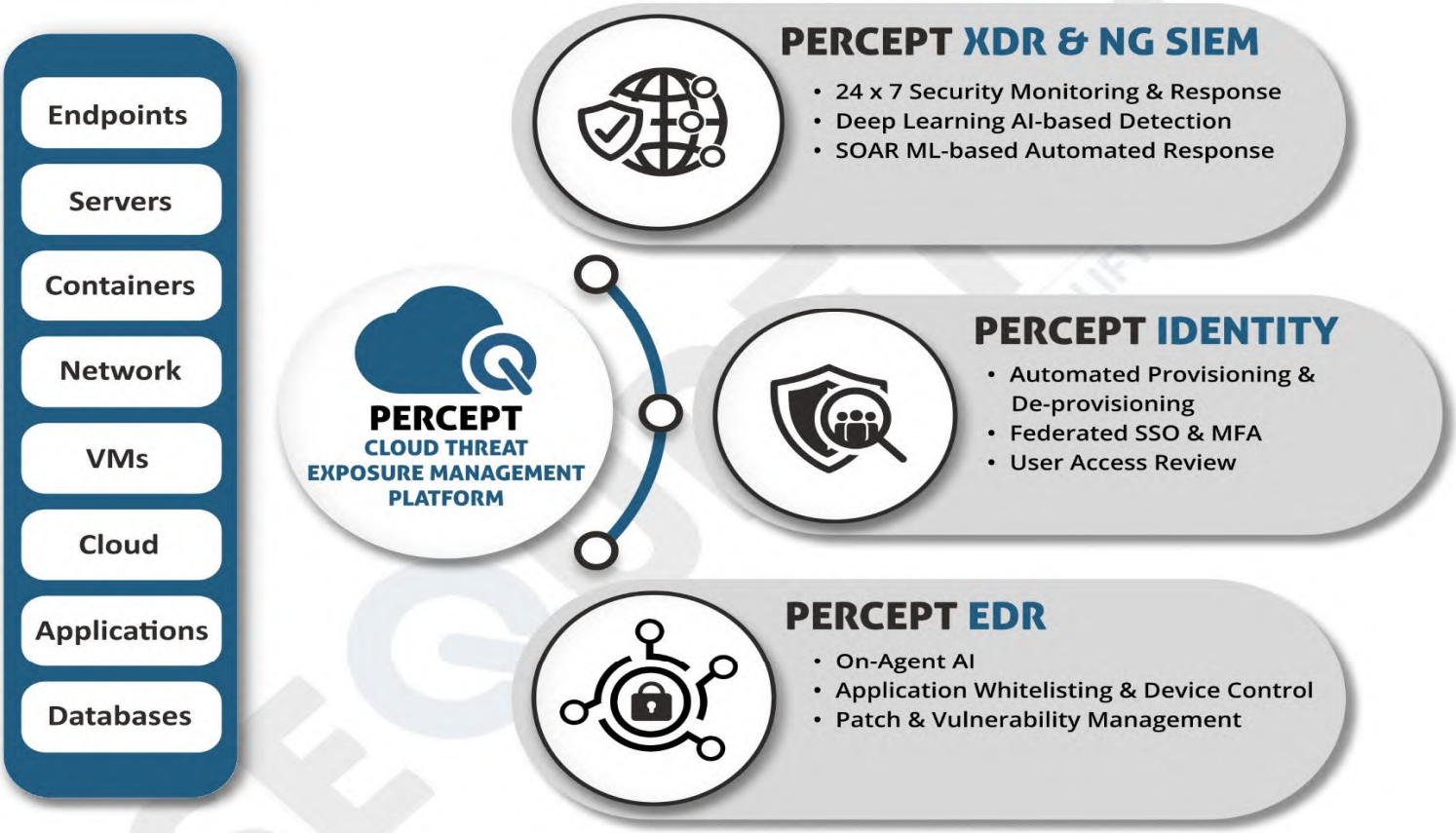
Technique Title	ID	Use
Commonly Used Port (T1043)	T1043	Cuttlefish communicates with the C2 server over commonly used ports like 443 for HTTPS, facilitating command and control operations.
Exfiltration		
Exfiltration Over Command and Control Channel (T1041)	T1041	Cuttlefish uploads compressed log files containing stolen data to the C2 server over the command and control channel.
Impact		
Data Destruction (T1485)	T1485	Cuttlefish can potentially be used to destroy data on compromised devices, impacting the integrity and availability of the network.

10 YEARS | SEQURETEK
SIMPLIFY SECURITY

Trusted by Global Customers, Investors, and Partners

About Sequretek

Sequretek is a global cybersecurity company that offers end-to-end security in the areas of enterprise threat monitoring, incident response, device security, identity & access governance through our own AI powered Percept Cloud Threat Exposure Management Platform.



Take Control of Your Enterprise Security

- Enterprise scale, easy to use, and cloud native
- AI-driven threat detection, protection, remediation, and response
- Quick implementation and integration capabilities
- End-to-End ownership and management of Sequretek products
- Reduced Total Cost of Ownership (TCO) while simplifying security
- Out-of-the-box reporting for compliance and audit purposes

Feel free to reach out to us at info@sequretek[.]com to know more about our products, or schedule a demo at https[:]//sequretek[.]com/request-a-demo/