Payatu

May 2022

Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

Table of Contents

01

Analysis of a RAT with Ransomware and DDOS-like Abilities, BoratRAT

Tags: Malware, RAT, Ransomware

Cyble Research Labs recently shared a blog about a new Remote Access Trojan called BoratRAT. With the provision of a dashboard for threat actors, BoratRAT assists threat actors in performing RAT activities, selecting one of the options from different categories like surveillance, control, malware, system control, bypass UAC, install; while compiling the binary so that attacks like DDOS and ransomware attacks.

Some of the major abilities of this RAT include Keylogger, Ransomware, DDOS, Audio Recording, Webcam Recording, Remote Desktop, Reverse Proxy, Process Hollowing, Browser Credential Stealing, Discord Token Stealing, and Remote activities.

For further details, refer to the complete blog by Cyble.

IOCs- Appendix 1A

02

Amid War, Anonymous Hacks Commercial Bank in Russia

Tags: Geopolitical, Financial, Bank, Energy Sector

In view of the geopolitical situations going on between Ukraine and Russia, the Anonymous hacker group has been attacking banks, energy sector companies under OpRussia. Sharing a massive amount of data (6TB) via DDoSecrets recently, Network Battalion 65, an affiliate of Anonymous hacked PSCB commercial bank in Russia, releasing 542GB archive containing 229,000 emails and 630,000 files.

Other companies breached include Elektrocentromontazh, a major power organization of Russia, and ALET – a customs broker for companies in the fuel and energy industries.

For further details, refer to leads from security affairs.

03

Phishing Campaign Themed on Chemical Attacks Used by JesterStealer Malware

Tags: Phishing, Malware, Stealer

Ukraine CERT has released an update wherein they identified mass distribution of malicious emails, themed on the topic of "chemical attack". This mail contains a link to an XLS document containing a macro that further downloads the exe file of JesterStealer.

Cryptowallets, password managers, messengers, Mail/VPN/FTP clients and other authentication data are targeted using JesterStealer and shared via statically defined proxy addresses in Telegram.

For further details, refer to the CERT-UA website.

IOCs – Appendix 1B

04

Critical Vulnerability in F5's BIG-IP Lets Unauthenticated User Execute Commands

Tags: Vulnerability, Infrastructure, F5, BIG-IP

CISA, the cyber security agency of the United States, updated on May 4th 2020 in its advisory, about a vulnerability in F5's BIG-IP. The vulnerability CVE-2022-1388 is defined as a control issue which allows an unauthenticated attacker with network access to the BIG-IP system through self IP addresses or via management port, can execute system commands, create/delete files and disable services arbitrarily. As of now the indicators of compromise shared by F5 mention entries in logs: **/var/log/audit, /var/log/restjavad-audit.0.log** which may display system commands request like for bash.

Other indicators suggest using F5 iHealth heuristics to detect unknown processes, iControl REST interface being exposed to the internet, and **Port Lockdown set to Allow All** for the self IP address. The list of affected products includes iControl REST in almost all modules 11.x through 17.x.

The fix for the same is available in the latest versions and for any further details, kindly refer to the advisory from F5.

Vulnerabilities

Critical

1. **CVE-2022-1388**

05

Arbitrary Code Execution in dotCMS Via Multipart File Directory Traversal

Tags: Bank, Vulnerability, Code Execution, Directory Traversal, Web-Application

While attempting to find bugs for a large bank, researchers have identified a possibility of Code Execution in dotCMS, this is possible via Content APIs in systems wherein CONTENT_APIS_ALLOW_ANONYMOUS is configured to WRITE, simply put, allowing anonymous users to write data via API.

Directory traversal occurs in dotCMS because it does not sanitize the filename passed as a multipart request. Through this uniquely crafted POST request, the files are uploaded by an anonymous user outside the temp directory. A jsp file to execute commands via cmd was exhibited by the researchers resulting in code execution.

This critical vulnerability has been resolved by team at dotCMS in versions 22.03, 5.3.8.10_lts, 21.06.7_lts. Another suggestion given by the team is to Disable Anonymous Content Submittal, where CONTENT_APIS_ALLOW_ANONYMOUS can be set to READ or NONE.

For further reference, kindly refer to dotCMS' advisory, and PoC available in the blog from the researchers.

06

CERT-In Issues Direction for Infosec Practices, and Reporting of Cyber Incidents

Tags: CERT-IN, Directive, Security Practices

In late April 2022, CERT-In, India's national agency for performing various functions in the area of cyber security, released a direction on "Information security practices, procedures, prevention, response and reporting of cyber incidents for Safe & Trusted Internet". In this direction, the agency identified certain gaps that were causing hindrances in incident analysis for any cyber incidents observed in an organization in India.

A quick review of key updates is shared below:

i. All ICT system clocks of "service providers, intermediaries, data centers, body corporate and government organizations" must be in synchronization with the NTP server of NIC (National Informatics Centre) or servers traceable to it.

ii. It is mandatory to report cyber incidents within 6 hours of noticing such incidents or being brought to notice about such incidents.

iii. Any organizations as mentioned in point (i), must take action on, and provide information for assistance of CERT-In and other organizations in mitigating cyber incidents. Also, every organization must assign a PoC (Point of Contact) who shall interact with CERT-In.

iv. Organizations must enable logs for all ICT systems and maintain them securely for a period of 180 days.

v. Data Service Providers, VPS (Virtual Private Server) Providers, Cloud Service Providers, VPN service providers shall maintain specific information related to their customers for a period of 5 years or longer even if the customer cancels

or withdraws the registration. This includes information like validated names, IPs allotted, Email address, IP address and time stamp of the customer at time of registration, validated contact and address details, ownership patterns of subscriber/customer and period of hire including dates.

vi. Any Virtual Asset Service Providers, Virtual Asset Exchange Providers and Custodian Wallet Providers shall maintain information obtained from KYC (Know Your Customer) and records of financial transactions for a duration of 5 years.

This direction is effective 60 days from its release, i.e., 28th April 2022.

For any further details, kindly refer to the direction from Cert-In.

07

China-based Espionage Group Targets Russian Officials Using PlugX Malware

Tags: Geopolitical, Malware, APT group, Ta416

Observing the shift in the political landscape since the beginning of the Russia-Ukraine War, the dynamics in the information security domain have also been observed to be changing. There has been a major impact on the collection requirements of threat actors, nation-backed actors, in order to benefit their country.

In a recent observation by researchers at SecureWorks, it has come to light that Bronze President, aka Mustang Panda, TA416, is a China-based cyber espionage group that is known to target government entities, non-profits, religious and other non-governmental organizations, has now been targeting Russian officials. Observed in a malicious executable file masquerading as a Russian language document.

For further details, kindly refer to SecureWorks' blog.

08

Nimbuspwn, A New Privilege Escalation in Linux

Tags: Vulnerability, Privilege Escalation, Linux, Nimbuspwn

Microsoft Defender Research team identified several vulnerabilities, collectively known as Nimbuspwn, that together are capable of elevating an attacker's privileges to root in a Linux desktop endpoint. Resulting in a number of attack vectors such as deploying backdoors, arbitrary RCE, and setting an initial foothold for deploying malware or ransomware.

Vulnerabilities CVE-2022-29799 (Directory Traversal) and CVE-2022-29800 (Time-of-check-time-of-use race condition), identified in a systemd unit called networkd-dispatcher, result in possible directory traversal, symlink race and other race condition issues could be leveraged to elevate privileges and deploy malwares. These vulnerabilities have now been fixed.

For further details on exploitation of the vulnerabilities, refer to Microsofts' security blog.

Vulnerabilities

High

1. **CVE-2022-29799**

Medium

1. **CVE-2022-29800**

09

CISA Releases Advisory Helping Organizations Defend Against Exploitation of Initial Access

Tags: CISA, Advisory, Initial Access, TTP, Security Practices

Weak security posture and security controls in the best of the organizations often lead to them being compromised and assist threat actors in gaining initial access to their network. CISA in its report assists the organizations in focusing on overlooked security controls and configurations which may allow a threat actor to gain access. These include configurations that are misconfigured or may be left unsecure.

Most common attack techniques that are used by threat actors include:
Exploitation of Public-Facing Applications [T1190], External Remote Services [T1133], Phishing [T1566], Trusted Relationship [T1199], Valid Accounts [T1078].

Explaining poor security controls and misconfigurations in detail, CISA highlighted some of the most common issues like, no use of MFA (Multi-Factor Authentication), incorrectly defined ACLs (Access Control List), vulnerable software or lack of patch management, usage of products with default config and default credentials, insufficient security controls on services like RDP and VPN, weak or no password policies, open ports and misconfigured services towards internet, insufficient controls to detect and block phishing attempts and most of all, poor EDR (Endpoint Detection and Response) applicability.

Mitigation Techniques:
The most important practices include adopting a Zero-trust policy, hardened access control policies, implementing MFA at critical access like VPN and public-facing applications, also monitoring the time of access and geolocation of IP accessing system is a good practice. Setting up SIEM and SOAR platforms for

log management and monitoring, efficient patch management policies that keep the systems up to date, antivirus, and prevention programs to block any malicious software.

For further reference or detailed insight, refer to CISAs' report.

10

Software Supply-Chain Attacks on The Rise

Tags: Supply-Chain Attack, NPM, Ruby, Rust, PyPI

Since the end of the previous year i.e., 2021, there have been multiple software supply-chain attacks. Some attacks resulted in major compromises and mass exploitation (for example, Log4j and Spring4shell vulnerabilities in different Java components), while some were identified in time with no major data breaches due to such supply-chain attacks.

The sudden rise in Supply-Chain attacks in April-May 2022 is massive, April 2022 gave us a vulnerability in NPM, wherein, npm allowed anyone to be added as a maintainer of the package without notifying the users, hence, a threat actor was able to masquerade a malicious package as a legitimate one, resulting in developers downloading the malicious package and, in some cases, even executing them as privileged user.

In the beginning of this month, May 2022, Rubygems published an advisory notifying user of a vulnerability that allowed unauthorized takeover of some gems, allowing user to remove and replace certain gems even if that user was not authorized to do so.

Another highlight of this month came from a security advisory by Rust, when they were notified by a user of a malicious crate named **"rustdecimal"** containing malware, which was published by a threat actor to target users "typosquatting" the legitimate crate - **"rust_decimal"**. With 500 downloads of the crate since

the time, it was released, the crate executed legitimate code similar to the original crate but had a function that set environment variables and downloaded a binary payload targeting Linux and macOS, but not Windows. Rust crate response team suggests periodic auditing of the dependencies and removal of the malicious dependency if found.

A similar technique of introducing a malicious package with lookalike name was attempted on PyPI, targeting **"PyKafka"** an Apache client package with **"Pymafka"** . This typo squat package reached 325 implementations providing initial access to a developer's internal environment. Python scripts and Cobalt Strike beacon were used for providing remote access capabilities. The package has been removed now, however, only a week later, another Python package **"ctx"** was in limelight due to very unusual activity, that is, version update after almost 7-8 years. Researchers at SANS ISC noticed this irregularity and going ahead with analysis of suspicious Python package update, identified that the package was trying to collect AWS-ACCESS-Key IDs and AWS secret Access keys from the environment variables and being posted on: hxxps://anti-theft-web[.]herokuapp[.]com/ In an update it has been claimed that this was done as a part of bug hunting activity by a security researcher.

11

VMWare Advises Customers to Patch Critical Vulnerabilities ASAP

Tags: VMWare, Advisory, Vulnerability, Infrastructure

VMWare released an advisory on May 18th 2022, informing its customer about two new vulnerabilities impacting its products. Both the vulnerabilities have been fixed, in addition, workaround of the Authentication Bypass vulnerability is available as well.

CVE-2022-22972, which is an Authentication Bypass vulnerability scored CVSS 9.8, may allow an attacker with network access to the UI to obtain administrative access without any authentication. The products affected include VMWare Workspace ONE Access, VMWare Identity Manager, VMware vRealize Automation. Also, an exploit of the vulnerability is being circulated publicly.

CVE-2022-22973, which is a Local Privilege Escalation Vulnerability scored CVSS 7.8, may allow an attacker with local access to escalate privileges to 'root'. The products affected include VMWare Workspace ONE Access, VMWare Identity Manager, VMware vRealize Automation.

Vulnerabilities

Critical

1. CVE-2022-22972

High

1. CVE-2022-22973

12

PDF Campaign Delivering Snake Keylogger

Tags: Malware, Campaign, KeyLogger

Researchers at HP have identified a pdf malware campaign that is observed to be delivering Snake Keylogger. Shared as an attachment to emails, the pdf pops up an alert on being opened in Adobe Reader, however, attackers have named the document "has been verified. However, pdf, jpeg, xlsx, docx", so that the alert seems to be a generic alert advising the user to be alert while opening such files and they could be potentially harmful to the computer.

The file on analysis is identified to store an embedded file which is of .docx format. If a user has disabled protected view option in Word format, the .rtf format file is downloaded onto the system from a domain – hxxps://vtaurl[.]com/lHytw.

On further analysis it is identified that the file and OLE objects stored in it, attempt to exploit CVE-2017-11882, an RCE in Equation Editor, via shellcode. This further downloads an exe file named, fresh[.]exe which is a Snake Keylogger executable.

IOCs – Appendix 1C

13

Critical Zoom Vulnerabilities Let Attacker Compromise Meetings by Just One Click

Tags: Zoom, Advisory, Vulnerability

Zoom is one of the most commonly used platforms for different online events, its applicability is not restricted to only professional discussions, but also for educational purposes, chats, webinars, and more. Recently, Zoom in its security bulletin disclosed four major vulnerabilities in its platform that could let an attacker spoof a user, trick them into downgrading to a less secure version, and trick users to connect to a malicious server instead of a legitimate one. Two of the vulnerabilities have been designated high severity, while the other two assigned medium severity.

CVE-2022-22784 – High, Improper XML Parsing in Zoom Client Meetings

This vulnerability allows an attacker to forge XMPP messages from the server by breaking out of the XMPP message context and create a new context to have receiving user's client platform to perform various actions. Vulnerability resides in Android, Linux, iOS, macOS, and Windows before version 5.10.0.

Vulnerabilities

High

1. CVE-2022-22784
2. CVE-2022-22786

Medium

1. CVE-2022-22785
2. CVE-2022-22787

CVE-2022-22785 – Medium, Improperly constrained session cookies in Zoom Client for Meetings

This vulnerability could allow an attacker to send a user's Zoom session cookies to a non-Zoom domain, and potentially spoof the user. Vulnerability identified in Android, Linux, iOS, macOS, and Windows before version 5.10.0.

CVE-2022-22786 – High, Update package downgrade in Zoom Client for meetings, for Windows

This vulnerability is caused due to improper validation of the version during the update process, resulting in an attacker tricking a user to downgrade their Zoom Client version to a less secure one. This vulnerability resides in Zoom Client for meetings in Windows.

CVE-2022-22787 – Medium, Insufficient hostname validation during server switch in Zoom Client for Meetings

This vulnerability is caused due to improper validation of the hostname during a server switch request, which can be used to trick a user client to connect to a malicious server when attempting to use Zoom services. Vulnerability resides in Android, Linux, iOS, macOS, and Windows before version 5.10.0.

14

Cisco Software Exploited in The Wild Using Zero-Day Vulnerability

Tags: Cisco, Vulnerability, Advisory, Zero-Day

Cisco published an advisory on May 20th, 2022, informing its customers of a zero-day identified in its IOS XR Software. The vulnerability is an Open Port vulnerability in its RPM software which allows an unauthenticated remote attacker to access the Redis instance that runs within its NOSi container.

When health check RPM is activated, it by default opens TCP port 6379, giving the attacker the ability to exploit the Redis instance by writing into the Redis in-memory database, and write arbitrary files to the container file system, collect information from the Redis database. However, it is not possible for the attacker to perform RCE or abuse the integrity of the host system.

The affected products include routers running Cisco IOS XR software release 7.3.3 which has been fixed in release 7.3.4

In case an organization is unable to apply fixes to their environment due to any reason, Cisco has also come along with workarounds. The first and most preferred one is to DISABLE health check, another effective technique that could be used of iACLs (Infrastructure Access Control Lists) to block port 6379. However, in case the traffic originates from a trusted source address, iACLs might be ineffective.

15

Appendix

Appendix 1: IOCs

Appendix 1A- BoratRAT

Hashes
d3559d9f1ca15f1706af9654fd2f4ccc
fb120d80a8c3e8891e22f20110c8f0aa59d1b036
d2ce3aa530ba6b6680759b79aa691260244ca91f5031aa9670248924cc983fb0
ddab2fe165c9c02281780f38f04a614e
2a5ad37e94037a4fc39ce7ba2d66ed8a424383e4
b47c77d237243747a51dd02d836444ba067cf6cc4b8b3344e5cf791f5f41d20e
3e645ccca1c44a00210924a3b0780955
5d8e8115489ac505c1d10fdd64e494e512dba793
f29e697efd7c5ecb928c0310ea832325bf6518786c8e1585e1b85cdc8701602f
f41bfa672cca0ec7a2b30ecebf7eac7e
d24d4fbd79967df196e77d127744659bbb2288d6
8c300944ae62e17ab05ad408c5fb5473ebccac514c8ddc17c47bc9fda451c91b
9726d7fe49c8ba43845ad8e5e2802bb8
8bcdf790826a2ac7adfc1e8b214e8de43e086b97
df31a70ceb0c481646eeaf94189242200fafd3df92f8b3ec97c0d0670f0e2259
7ee673594bbb20f65448aab05f1361d0
2a29736882439ef4c9088913e7905c0408cb2443
8fa7634b7dca1a451cf8940429be6ad2440821ed04d5d70b6e727e5968e0b5f6

Hashes
62c231bafa469ab04f090fcb4475d360
62c231bafa469ab04f090fcb4475d360
82dda56bc59ac7db05eddbe4bcf0fe9323e32073
6a4f32b0228092ce68e8448c6f4b74b4c654f40fb2d462c1d6bbd4b4ef09053d
4ccd3dfb14ffdddfa598d1096f0190ea
c68c30355599461aca7205a7cbdb3bb1830d59c8
7f8a306826fcb0ee985a2b6d874c805f7f9b2062a1123ea4bb7f1eba90fc1b81
0b7c33c5739903ba4f4b78c446773528
b58555bebddf8e695880014d34a863a647da547e
2d9625f41793f62bfe32c10b2d5e05668e321bcaf8b73414b3c31ef677b9bff4
499fc6ac30b3b342833c79523be4a60c
dcf1ed3fbc56d63b42c88ede88f9cad1d509e7ec
dcac599b1bab37e1a388ac469e6cc5de1f35eb02beaa6778f07a1c090ce3ea04
87651b12453131dafd3e91f60d8aef5a
d5db880256bffa098718894edf684ea0dc4c335d
a15d72d990686d06d89d7e11df2b16bcd5719a40298c19d046fa22c40d56af44
0cd62cd02962be20ed92abcd0c9e9a25
69fbadc8a4461413c30cd0579d89f8668187e5a2
5c124a7e35025d3e94df6b17dca5332e9a5aaabdca2355c113f3c93b572281b7
a45679bdcf30f068032bd37a194fa175
f23fd98f28bb0b482f0aae028172e11536e4688c

Hashes
16beb1ae2de2974ccc2371d9f619f492295e590abb65d3102e362c8ec27f2bbb
872145b37d107144894c9aa8729bad42
01610587bcfa7ac379b1f0169a2a9ab384b9116b
2f258949fd95da6cd912beb7203a9fd5e99d050309a40341de67537edb75aadc
590b00c87d5ff2ffe09079f0406eb2cd
92c91f1db8c2c8cc34c2e1a26f4f970f1518a7ed
adb00dee751b4ba620d3b0e002f5b6d8b89cf63b062f74ec65bba72294d553d1
509d41da4a688a2e50fc8e3afca074c7
228de17938071733585842c59ffb99177831b558
f91973113fd01465999ce317f3e7a89df8c91a5efadcfa61e5ccce687bf3580a
509d41da4a688a2e50fc8e3afca074c7
228de17938071733585842c59ffb99177831b558
f91973113fd01465999ce317f3e7a89df8c91a5efadcfa61e5ccce687bf3580a
12911f5654d6346fe99ef91e90849c13
1b8e63d03feb84d995c02dcbb74da7edfaa8c763
7eed1b90946a6db1fe978d177a80542b5db0bf3156c979dc8a8869a94811bf4b
3a474b8dee059562b31887197d94f382
b31455f9583b89cac9f655c136801673fb7b4b9a
c9b8e795c5a024f9e3c85ba64534b9bf52cc8c3d29b95ff6417dc3a54bc68b95
91edcb945924df5fbf4ff123aa63199c
d124869aaee9aa1a49def714774b834335aa746e

Hashes
5b1f80ff787bdcd7ee12aa64be1f2f5f1f658bd644bbc5fd73527b51da6ce0d6
ef998529d037fcdb2bde6d046f99db45
1a38a1182155429ecc64c20ece46ec0836c32ec7
54f554b9e330476b3903756f62b577bab35cdef941d3d0f6a3d607862762bf91
ea1ff113b847312d57fa8621f71f460f
535a4e525da7e98f4f4f69abc923a1065bd2d3fa
58f9e3c90446dfecfec64221eb11167dd41d0e8dedda2ea9f83d9dda2890e6f3
8749c78b8ad09a3b240dd1384a17539b
b9263ac725ccd8c664ae0f9da5fc0d00adcb8c5e
657e3f1f449c0b710b0c571ec8eee689ae16793fb63b996e0182420d768f89bd
acbf0f8b09320f3e967ee83fcda26f5d
bbee0fa1c88edcd0469974223fb026e1176256dc
203300be75ad8f57972324519b2583a44e759cdd57390d6765df10288e249789
0f93650dd78557f41b7c5467e3b6b6a7
382bd4496eb7439fde85832abca87cc21cb7872f
cc5b49d2a2821d4f6ef6af8a1e50994c6690d6a4daa41bd048fe79bd8b578988
e89a0b897f93d7d5cb433b3fd01764c9
9e72e85d13fe70c2518041e30d202f04b14324b6
d8a115310142f2e874dc7ea2a393fada679838bddb87f4cfd9aaef631641cb72
7f3a6c23c979f840d98b8b04a583cde9
941c50a425479c5f025fbb152a1a0754ac03c252

Hashes
0da1bd8e67d6f499cc3b296fc278103497f7ca2f692fe76e3c0413b0e14df777
d405b02cb6c624a7df4ebecefc5d23a9
0272d8cc3456a9bdfff7431f9ce238c93511cacd
e06a66122af82580a883ce21609f89628e5dd648726307693d398c0661a1e5c1

Appendix 1B - JesterStealer

Md5	SHA	filename
d5c9fd40738ac33f59467811c1ceb30b	5df051b418cd3d51cfcfe17685275e03b0efdf9a80ce237d2deccb3749576092	Map023.xlsb
d80f1d64e07909d29d7a2a1888931af9	f963ed8559ade984e81a95238c4875d4c0a6ff14a7695630429bf98d4235d596	Map021.xlsb
4742c9d0a6b5b3b10ae7eb8f6b3e2fe6	ef7ddd544267a8781c99f08146d455aa08beab867e0453b07f1131edcbef92b2	Map026.xlsb
70ef45cb31af0b6f37be051de4170839	a2234ee40097fa832eb3a533840e86de3933cf216fbf8445d2946cb7b61c887b	Updater-Microsoft.exe
8f32a69ecd777f99d67bd18363afa25d	da0de03004e3ec2711ddc71e119ecc252568b2c9300b98dd2434b8e83ce02dc9	a1.exe
31600c8891e3902a0fe2d2985d25ca34	f7477c153f861d8c57d4794481445134426d634b9f4ca58d4d8519c4b0cd0085	ckloc (JesterStealer)

Network
tachikawaobs@sv5206.xserver.jp
157 [.] 112.183.47
igshop [.] net (Compromised Web Resource)
dcshost [.] net (Compromised Web Resource)

Network
lightnogu5owjjllyo4tj2sfos6fchnmcidlgo6c7e6fz2hgryhfhoyd [.] onion
wasabiwallet [.] online
ip-api [.] com (Legitimate service)
hxxps://igshop[.]net/uploads/Map026.xlsb
hxxps://igshop[.]net/uploads/Map023.xlsb
hxxps://igshop[.]net/uploads/Map021.xlsb
hxxps://igshop[.]net/uploads/Updater-Microsoft.exe
hxxps: // dcshost [.] net / mail / OfficeUpdaterNew.exe
hxxps: //marmaris.com [.] ua / misc / Updater-Microsoft.exe
hxxps: //autodoka.com [.] ua / extra / Updater-Microsoft.exe
hxxp: // lightnogu5owjjllyo4tj2sfos6fchnmcidlgo6c7e6fz2hgryhfhoyd [.] onion / stealer / 1026977440
hxxp: // ip-api [.] com / json (Legitimate service)
tcp: // wasabiwallet [.] online: 7777

Appendix 1C – Snake KeyLogger

Hashes
05dc0792a89e18f5485d9127d2063b343cfd2a5d497c9b5df91dc687f9a1341d
250d2cd13474133227c3199467a30f4e1e17de7c7c4190c4784e46ecf77e51fe
165305d6744591b745661e93dc9feaea73ee0a8ce4dbe93fde8f76d0fc2f8c3f
297f318975256c22e5069d714dd42753b78b0a23e24266b9b67feb7352942962
f1794bfabeae40abc925a14f4e9158b92616269ed9bcf9aff95d1c19fa79352e
20a3e59a047b8a05c7fd31b62ee57ed3510787a979a23ce1fde4996514fae803

Domains
hxxps://vtaurl[.]com/lHytw
hxxp://192.227.196[.]211/tea_shipping/f_document_shp.doc
hxxp://192.227.196[.]211/FRESH/fresh.exe
mail.saadzakhary[.]com:587

Appendix 2

MITRE Techniques – BoratRAT

Tactic	Technique ID	Technique Name
Execution	T1204	User Execution
Discovery	T1518	Security Software Discovery
	T1087	Account Discovery
	T1083	File and Directory Discovery
Collection	T1123	Audio Capture
	T1005	Data from Local System
	T1056 .001	Keylogging
	T1113	Screen Capture
	T1125	Video Capture
Command and Control	T1132	Data Encoding
	T1219	Remote Access Software
Exfiltration	T1020	Automated Exfiltration
Impact	T1485	Data Destruction
	T1486	Data Encrypted for Impact
	T1565	Data Manipulation
	T1499	Endpoint Denial of Service

Payatu's Security Capabilities

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

Web Security Testing

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

Product Security

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components "fit" together in your mega-product.

Mobile Security Testing

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.

Cloud Security Assessment

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared responsibility to secure the information stored in their cloud. Payatu's expertise in cloud

protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.

Code Review

Payatu's Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.

Red Team Assessment

Red Team Assessment is a goal-directed, multi-dimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization's crown jewels and test its readiness to detect and withstand a targeted attack.

More Services Offered by Payatu -

- IoT Security Testing
- AI/ML Security Audit
- DevSecOps Consulting
- Critical Infrastructure
- Trainings