Payatu

June 2022

# Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

## Table of Contents

01

# CVE-2022-30190 aka Follina Actively Exploited by Attackers in the Wild

**Tags:** CVE-2022-30190, Follina, Zero-day, Vulnerability

Microsoft in its security update released a zero-day vulnerability that exists in MSDT – Microsoft Windows Support Diagnostic tool. The vulnerability is an RCE (Remote Code Execution). When an application such as Word, or PowerPoint uses URL protocol, it calls MSDT (Microsoft Support Diagnostic Tool), here, an attacker runs arbitrary code with the privileges of the calling application. Through this vulnerability, an attacker can install programs, view, change or delete data and create new accounts as per the privileges of the user rights.

The vulnerability compromises all three principles of information security - Confidentiality, Integrity and Availability. Proofpoint researchers shared via twitter that they have identified malicious emails containing fake recruitment documents from various companies. These mails have been observed targeting US and EU governments and are delivered via Qbot malware.

The patch for this vulnerability has been published along with 55 other vulnerabilities by Microsoft in its June cumulative updates or Patch Tuesday batch.

**CVSS Score – 7.0 (High)**

**For further details on the vulnerability, kindly refer to Microsoft's Update guide.**

02

# Cyber Attack on a Nigerian Bank Through Insider Threat Averted

**Tags:** Insider Threat, Banking/Finance, Nigeria, Fraud

Nigerian Police Special Fraud Unit (PSFU), posted the arrest of members of a syndicate that planned to launch cyber-attacks and siphon huge amount of money. The MO (Modus Operandi) of the group was Insider Threat, wherein one of the attackers, who was also an ex-staff member of IT department of one of the leading Nigerian Banks, attempted to hire a current employee from IT department, who would go on and purposely keep critical gateways and ports open on the bank's server so that the syndicate could access the application and network, moving out money from the network using Python application and Zoom (A Video Conferencing Platform).

Going further with the investigation, the forensic analysis of electronic devices possessed by these attackers, revealed that they were planning a similar attack on 10 different banks once the initial attack was successful.

Insider Threat or Insider Attack is a major issue that the financial sector has been observing in recent years. Since the compromise of banks focuses on high and one-time monetary success, it is quite prominent to include an insider with critical levels of permissions, such as privileged users and administrators, third-party workers, etc. with access to critical infrastructures and sensitive data. For such cases,

- It is highly important to have a background check, multiple levels of verification of such employees,
- Since insider threat is very tough to identify, regular activity checks of employees are advisable,
- Real-time monitoring of critical infrastructures, a well-defined procedure with Change Management must be included and maintaining ACLs (Access Control Lists) with stringent whitelisting and blocking procedures is equally important.

03

# A Brief Background of HelloXD Ransomware

**Tags:** Ransomware, HelloXD, IOC

Surfacing in November 2021, the HelloXD ransomware family has been observed targeting Windows and Linux variants. The malware family uses a modified ClamAV logo for executables, and on execution attempts to disable shadow copies so that it looks like system recovery, followed by encryption of files. In addition, the ransomware also sends an outbound connection through a ping command which contains a timeout of 3000 milliseconds and a command to delete the initial payload.

Once the ransomware encrypts the files, a ransom note containing an onion link and a TOX ID (Tox, a P2P Instant messaging app) for the victim, along with instructions to the victim to install for connecting to the attacker and getting a decryption method.

**For IOCs – Appendix 1A**

**For a detailed report, refer to Palo Alto's report.**

04

# Implications of India's New Data Regulation Law, VPN Provider Shuts Servers in India

**Tags:** CERT-IN, VPN, Data Regulation Law

On April 28th, 2022, CERT-IN released a set of directions updating data regulation laws in India, revising its policy for VPN service providers, which instructs them to mandatorily enable customer logs for 180 days, and store customer data such as IP addresses allotted, the purpose of hiring services, and email addresses for a duration of 5 years.

In response to this directive, Surfshark, a popular VPN service provider has decided to go ahead and shut down its servers existing in India. According to the company, a 'no logs' policy is one of the core ethos, and it is the opposite of one of the principles of VPN, that is privacy.

As a next step to manage Indian users, the company plans to setup virtual servers for India, which will physically be based in Singapore and London, but will be available as Indian servers in the list of servers.

05

# FDA-US and CISA Release Critical Advisory on Illumina's Sequencing Instruments

**Tags:** Vulnerability, Illumina products, Healthcare, Public Health

CISA (Cybersecurity & Infrastructure Security Agency – the U.S.), released an advisory on June 2nd, 2022 (ICSA-22-153-02) regarding vulnerabilities in a software used in Illumina sequencing instruments.; used in sequencing DNA or testing for genetic conditions, or for research only. These instruments are operable in dual boot modes namely, clinical diagnostic mode and RUO (Research Use Only) mode.

The vulnerability exists in LRM (Local Run Manager) software that runs on elevated privileges and is vulnerable to – Path Traversal, Unrestricted File Upload, Improper Access Control and Cleartext Transmission of sensitive data. Since it runs on elevated privileges, any attacker who has exploited the system via Path Traversal or Unrestricted File Upload can directly execute the code remotely at Operating System levels, and also modify system settings.

## THE ILLUMINA PRODUCTS USING VULNERABLE SOFTWARE

1. NextSeq 550Dx
2. MiSeq Dx
3. NextSeq 500 (ROU mode)
4. MiSeq (ROU mode)
5. iSeq 100 (ROU mode)
6. MiniSeq (ROU mode)

06

# Aoqin Dragon Spies on SouthEast Asian Countries Almost Ten Years Through Public Vulnerabilities

**Tags:** China, APT Group, Aoqis Dragon, Government, Education, Telecommunication, South East Asia, Australia

China linked APT group - "Aoqin Dragon" has been identified by SentinelOne to be spying on Telecom, Education, and Government sectors in Southeast Asian countries like Cambodia, Hong Kong, Singapore, Vietnam, and also Australia. Active probably since 2013, the threat group has been gaining access to various victims through phishing (T1566, especially through T1566.001), replicating data through removable Media (T1091) into such organizations, and also attempting to exploit unpatched vulnerabilities on public-facing applications (T1190), like CVE-2012-0158 and CVE-2010-3333.

Once these attackers gain initial access to an organization, dropper files tend to download executables mainly constituting Mongall backdoor and modified Heyoka backdoors. These malwares use techniques like DLL-hijacking, use of obfuscated-files, and DNS tunneling for defense-evasion of the system. These malwares are also composed of spreader components, which further look for any removable disks connected to the compromised system for further spreading the malware to other systems.

**For IOCs- Appendix 1B**

**For a detailed analysis, kindly refer to SentinelOne Labs' report.**

07

# PACMAN, A Novel Hardware Attack

**Tags:** Hardware, Exploitation, Apple products

Researchers at MIT-CSAIL (Computer Science and Artificial Intelligence Laboratory) discovered an attack technique in the Apple M1 CPU, that can compromise a system without any physical access. Existing between software attacks, like the Memory Corruption attack, and hardware attacks, like Microarchitectural Side Channels, PACMAN is an exploitation technique in which an attacker bypasses Pointer Authentication Codes (PAC) on Apple M1 CPU.

Pointer Authentication Codes are used in arm64e architectures to detect and guard against any unusual changes that might be made to the pointers in memory. These codes or cryptographic signatures are added to unused high-order bits of a pointer before storing the pointer. In case any malicious application or process attempts to set a high-order bit in the pointer, it will be interpreted as an authentication failure as memory corruption and the application will crash.

**For further details on the PACMAN attack, kindly refer to the PACMAN attack's website.**

08

# Another Action by Law Enforcement Agencies, Leak Websites Taken Down

**Tags:** Law Enforcement Agency, Takedown, Leak Market, Leak Websites, DDOS

US Law Enforcement Agencies seized another leak market/forum - weleakinfo[.]to and 2 related domains namely, ipstress[.]in and ovh-booter[.]com. These sites were used for selling hacked personal information and also supported DDOS (Distributed Denial of Service) attacks.

Shared on the DOJ's (Department of Justice) website, the news contains details about the activities of threat actors and the website (weleakinfo[.]to). The website acted as a search engine for its users to review and obtain PII (Personal Identifiable Information) of data from over 10,000 data breaches, which contained more than 7 billion indexed records, inclusive of names, email addresses, usernames, phone numbers, passwords and online accounts.

The other two websites publicly offered their clients to perform DDOS attacks on targets specified, through booter and stressor attacks. These seizures were part of a joint operation between the FBI, the DOJ, the National Police Corps of Netherlands, and the Federal Police of Belgium.

09

# Major Security Update by MEGA, the Cloud Storage Service

**Tags:** MEGA, Cloud, Cloud Security, Storage, Vulnerability

MEGA through its official website, shared a security update, informing its users about a critical vulnerability in its cryptographic architecture. The vulnerability identified along with four others, was shared by researchers at ETH Zurich. The attack vector here required an attacker to have control of the MEGA's API back-end or mount a TLS MITM (Man-In-The-Middle Attack) to compromise the End-to-End Encryption (E2EE) provided by MEGA.

Once the above-mentioned requirements were complete, it was possible to incrementally collect information every time a user logged in to their MEGA account. After a minimum of 512 logins through an account, it was also possible for an attacker to decrypt further information and parts of the account. These two vulnerabilities compromised the integrity of user credentials and ciphertext, keys used, ultimately compromising the privacy and integrity of an entire account (marked as 3rd Vulnerability).

The 4th vulnerability allowed an attacker to insert arbitrary files into a user's account if they had access or knowledge of any file link that had been exported via their account (Highly Critical), compromising the integrity of files. The final vulnerability is an issue in the mechanism of Legacy Chat Key Exchange (in the RSA mechanism to be precise), resulting in a Bleichenbacher-style attack (attack requires a high number of client interactions to compromise the integrity of a user).

The first 3 vulnerabilities have been fixed and released for clients on: Webclient, iOS App, Android App, MEGA Desktop App, MEGA CMD, and MEGA on NAS. The 4th vulnerability is to be fixed in coming releases, while the legacy code used for the 5th vulnerability will be removed in future releases.

10

# ToddyCat APT Group Targets Organizations in Europe and Asia

**Tags:** APT, Asia, Europe

ToddyCat is a threat actor, operational since December 2020, and has been observed to be targeting multiple high-profile organizations in Asia and Europe. Previously identified to target its victims via tools like Samurai Backdoor and Ninja Trojan, the actor compromises exchange servers in Taiwan and Vietnam, leading to multi-stage infection chains.

The actor also exploited ProxyLogon vulnerability, when it was identified in March 2021, targeting and compromising multiple organizations across Europe and Asia. Samurai Backdoor, a backdoor written in C#, connects through ports 80 and 443 allowing the attacker to administer the remote system and move laterally inside the victim's network. Similarly, Ninja too, is used for post-exploitation techniques like remote administrative control, and evading detections. It also uses features similar to Cobalt Strike, like pivot listeners and Malleable C2 Profile and is also known for infecting machines by sending malicious loaders via Telegram.

**For IOCs, refer to Appendix 1C**

**For further detailed analysis, refer to the report by KasperSky.**

11

# Major Ransomware Attack Claims of the Month

01 LockBit2.0 ransomware claimed to have compromised Mandiant (Cyber Defense Solutions company) on June 06th, 2022.

02 Cuba ransomware claimed to have compromised ETron Technologies (Taiwanese IC designing company) on June 13th, 2022.

03 LockBit2.0 ransomware claimed to have compromised Kuwait Airways on June 27th, 2022.

04 RansomHouse ransomware claimed to have compromised AMD (Advanced Micro Devices - an American multinational semiconductor company) leaking 450GB of data on June 28th, 2022.

## Appendix 1 - IOCs

### Appendix 1A- HelloXD Ransomware

| SHA |
| --- |
| 435781ab608ff908123d9f4758132fa45d459956755d27027a52b8c9e61f9589 |
| ebd310cb5f63b364c4ce3ca24db5d654132b87728babae4dc3fb675266148fe9 |
| 65ccbd63fbe96ea8830396c575926af476c06352bb88f9c22f90de7bb85366a3 |
| 903c04976fa6e6721c596354f383a4d4272c6730b29eee00b0ec599265963e74 |
| 7247f33113710e5d9bd036f4c7ac2d847b0bf2ac2769cd8246a10f09d0a41bab |
| 4e9d4afc901fa1766e48327f3c9642c893831af310bc18ccf876d44ea4efbf1d |
| 709b7e8edb6cc65189739921078b54f0646d38358f9a8993c343b97f3493a4d9 |

## Appendix 1B - Aoqin Dragon IOCs

### Hashes:

| SHA1 | Malware |
|---|---|
| a96caf60c50e7c589fefc62d89c27e6ac60cdf2c | Mongall |
| ccccf5e131abe74066b75e8a49c82373414f5d95 | Mongall |
| 5408f6281aa32c02e17003e0118de82dfa82081e | Mongall |
| a37bb5caa546bc4d58e264fe55e9e9155f36d9d8 | Mongall |
| 779fa3ebfa1af49419be4ae80b54096b5abedbf9 | Mongall |
| 2748cbafc7f3c9a3752dc1446ee838c5c5506b23 | Mongall |
| eaf9fbddf357bdcf9a5c7f4ad2b9e5f81f96b6a1 | Mongall |
| 6380b7cf83722044558512202634c2ef4bc5e786 | Mongall |
| 31cddf48ee612d1d5ba2a7929750dee0408b19c7 | Mongall |
| 677cdfd2d686f7148a49897b9f6c377c7d26c5e0 | Mongall |
| 911e4e76f3e56c9eccf57e2da7350ce18b488a7f | Mongall |
| c6b061b0a4d725357d5753c48dda8f272c0cf2ae | Mongall |
| dc7436e9bc83deea01e44db3d5dac0eec566b28c | Mongall |
| 5cd555b2c5c6f6c6c8ec5a2f79330ec64fab2bb0 | Mongall |
| 668180ed487bd3ef984d1b009a89510c42c35d06 | Mongall |
| 28a23f1bc69143c224826962f8c50a3cf6df3130 | Mongall |
| ab81f911b1e0d05645e979c82f78d92b0616b111 | Mongall |
| 47215f0f4223c1ecf8cdeb847317014dec3450fb | Mongall |
| 061439a3c70d7b5c3aed48b342dda9c4ce559ea6 | Mongall |
| aa83d81ab543a576b45c824a3051c04c18d0716a | Mongall |

| SHA1 | Malware |
|---|---|
| 43d9d286a38e9703c1154e56bd37c5c399497620 | Mongall |
| 435f943d20ab7b3ecc292e5b16683a94e50c617e | Mongall |
| 94b486d650f5ca1761ee79cdff36544c0cc07fe9 | Mongall |
| 1bef29f2ab38f0219b1dceb5d37b9bda0e9288f5 | Mongall |
| 01fb97fbb0b864c62d3a59a10e785592bb26c716 | Mongall |
| 03a5bee9e9686c18a4f673aadd1e279f53e1c68f | Mongall |
| 1270af048aadcc7a9fc0fd4a82b9864ace0b6fb6 | Mongall |
| e2e7b7ba7cbd96c9eec1bcb16639dec87d06b8dd | Mongall |
| 08d22a045f4b16a2939afe029232c6a8f74dcde2 | Mongall |
| 96bd0d29c319286afaf35ceece236328109cb660 | Mongall |
| 6cd9886fcb0bd3243011a1f6a2d1dc2da9721aec | Mongall |
| 271bd3922eafac4199322177c1ae24b1265885e8 | Mongall |
| e966bdb1489256538422a9eb54b94441ddf92efc | Mongall |
| 134d5662f909734c1814a5c0b4550e39a99f524b | Mongall |
| 134d5662f909734c1814a5c0b4550e39a99f524b | Mongall |
| 93eb2e93972f03d043b6cf0127812fd150ca5ec5 | Mongall |
| a8e7722fba8a82749540392e97a021f7da11a15a | Mongall |
| 436a4f88a5c48c9ee977c6fbcc8a6b1cae35d609 | Mongall |
| ab4cd6a3a4c1a89d70077f84f79d5937b31ebe16 | Mongall |
| 8340a9bbae0ff573a2ea103d7cbbb34c20b6027d | Mongall |
| 31b37127440193b9c8ecabedc214ef51a41b833c | Mongall |
| ed441509380e72961b263d07409ee5987820d7ae | Mongall |

| SHA1 | Malware |
|---|---|
| 45d156d2b696338bf557a509eaaca9d4bc34ba4a | Mongall |
| bac8248bb6f4a303d5c4e4ce0cd410dc447951ea | Mongall |
| 15350967659da8a57e4d8e19368d785776268a0e | Mongall |
| 008dd0c161a0d4042bdeb1f1bd62039a9224b7f0 | Mongall |
| 7e1f5f74c1bf2790c8931f578e94c02e791a6f5f | Mongall |
| 16a59d124acc977559b3126f9ec93084ca9b76c7 | Mongall |
| 38ba46a18669918dea27574da0e0941228427598 | Mongall |
| 38ba46a18669918dea27574da0e0941228427598 | Mongall |
| 19814580d3a3a87950fbe5a0be226f9610d459ed | Mongall |
| d82ebb851db68bce949ba6151a7063dab26a4d54 | Mongall |
| 0b2956ad5695b115b330388a60e53fb13b1d48c3 | Mongall |
| 7fb2838b197981fbc6b5b219d115a288831c684c | Mongall |
| af8209bad7a42871b143ad4c024ed421ea355766 | Mongall |
| 72d563fdc04390ba6e7c3df058709c652c193f9c | Mongall |
| db4b1507f8902c95d10b1ed601b56e03499718c5 | Mongall |
| f5cc1819c4792df19f8154c88ff466b725a695f6 | Mongall |
| 86e04e6a149fd818869721df9712789d04c84182 | Mongall |
| a64fbd2e5e47fea174dd739053eec021e13667f8 | Mongall |
| d36c3d857d23c89bbdfefd6c395516a68ffa6b82 | Mongall |
| d15947ba6d65a22dcf8eff917678e2b386c5f662 | Mongall |
| 5fa90cb49d0829410505b78d4037461b67935371 | Mongall |
| f2bf467a5e222a46cd8072043ce29b4b72f6a060 | Mongall |

| SHA1 | Malware |
|---|---|
| e061de5ce7fa02a90bbebf375bb510158c54a045 | Mongall |
| 4e0b42591b71e35dd1edd2e27c94542f64cfa22f | Mongall |
| 330402c612dc9fafffca5c7f4e97d2e227f0b6d4 | Mongall |
| 5f4cd9cd3d72c52881af6b08e58611a0fe1b35bf | Mongall |
| 2de1184557622fa34417d2356388e776246e748a | Mongall |
| 9a9aff027ad62323bdcca34f898dbcefe4df629b | Mongall |
| 9cd48fddd536f2c2e28f622170e2527a9ca84ee0 | Mongall |
| 2c99022b592d2d8e4a905bacd25ce7e1ec3ed3bb | Mongall |
| 69e0fcdc24fe17e41ebaee71f09d390b45f9e5c2 | Mongall |
| a2ea8a9abf749e3968a317b5dc5b95c88edc5b6f | Mongall |
| 0a8e432f63cc8955e2725684602714ab710e8b0a | Mongall |
| 309accad8345f92eb19bd257cfc7dd8d0c00b910 | Mongall |
| 89937567c575d38778b08289876b938a0e766f14 | Mongall |
| 19bd1573564fe2c73e08dce4c4ad08b2161e0556 | Mongall |
| a1d0c96db49f1eef7fd71cbed13f2fb6d521ab6a | Mongall |
| 936748b63b1c9775cef17c8cdbba9f45ceba3389 | Mongall |
| 46d54a3de7e139b191b999118972ea394c48a97f | Mongall |
| 4786066b29066986b35db0bfce1f58ec8051ba6b | Mongall |
| b1d84d33d37526c042f5d241b94f8b77e1aa8b98 | Mongall |
| 7bb500f0c17014dd0d5e7179c52134b849982465 | Mongall |
| d1d3219006fdfd4654c52e84051fb2551de2373a | Mongall |
| 0ffa5e49f17bc722c37a08041e6d80ee073d0d8f | Mongall |

| SHA1 | Malware |
|---|---|
| dceecf543f15344b875418ad086d9706bfef1447 | Mongall |
| fa177d9bd5334d8e4d981a5a9ab09b41141e9dcc | Mongall |
| 07aab5761d56159622970a0213038a62d53743c2 | Mongall |
| d83dde58a510bdd3243038b1f1873e7da3114bcf | Mongall |
| a0da713ee28a17371691aaa901149745f965eb90 | Mongall |
| c5b644a33fb027900111d5d4912e28b7dcce88ff | Mongall |
| db5437fec902cc1bcbad4bef4d055651e9926a89 | Mongall |
| ff42d2819c1a73e0032df6c430f0c67582adba74 | Mongall |
| 3b2d858c682342127769202a806e8ab7f1e43173 | Mongall |
| c08bf3ae164e8e9d1d9f51dffcbe7039dce4c643 | Mongall |
| f41d1966285667e74a419e404f43c7693f3b0383 | Mongall |
| 3ccb546f12d9ed6ad7736c581e7a00c86592e5dd | Mongall |
| 904556fed1aa00250eee1a69d68f78c4ce66a8dc | Mongall |
| bd9dec094c349a5b7d9690ab1e58877a9f001acf | Mongall |
| 87e6ab15f16b1ed3db9cc63d738bf9d0b739a220 | Mongall |
| f8fc307f7d53b2991dea3805f1eebf3417a7082b | Mongall |
| ece4c9fc15acd96909deab3ff207359037012fd5 | Mongall |
| 7fdfec70c8daae07a29a2c9077062e6636029806 | Mongall |
| 17d548b2dca6625271649dc93293fdf998813b21 | Mongall |
| 6a7ac7ebab65c7d8394d187aafb5d8b3f7994d21 | Mongall |
| fee78ccadb727797ddf51d76ff43bf459bfa8e89 | Mongall |
| 4bf58addcd01ab6eebca355a5dda819d78631b44 | Mongall |

| SHA1 | Malware |
|---|---|
| fd9f0e40bf4f7f975385f58d120d07cdd91df330 | Mongall |
| a76c21af39b0cc3f7557de645e4aaeccaf244c1e | Mongall |
| 7ff9511ebe6f95fc73bc0fa94458f18ee0fb395d | Mongall |
| 97c5003e5eacbc8f5258b88493f148f148305df5 | Mongall |
| f92edf91407ab2c22f2246a028e81cf1c99ce89e | Mongall |
| d932f7d11f8681a635e70849b9c8181406675930 | Mongall |
| b0b13e9445b94ed2b69448044fbfd569589f8586 | Mongall |
| b194b26de8c1f31b0c075ceb0ab1e80d9c110efc | Mongall |
| df26b43439c02b8cd4bff78b0ea01035df221f68 | Mongall |
| 60bd17aa94531b89f80d7158458494b279be62b4 | Mongall |
| 33abee43acfe25b295a4b2accfaf33e2aaf2b879 | Mongall |
| c87a8492de90a415d1fbe32becbafef5d5d8eabb | Mongall |
| 68b731fcb6d1a88adf30af079bea8efdb0c2ee6e | Mongall |
| cf7c5d32d73fb90475e58597044e7f20f77728af | Mongall |
| 1ab85632e63a1e4944128619a9dafb6405558863 | Mongall |
| 1f0d3c8e373c529a0c3e0172f5f0fb37e1cdd290 | Mongall |
| f69050c8bdcbb1b5f16ca069e231b66d52c0a652 | Mongall |
| 6ff079e886cbc6be0f745b044ee324120de3dab2 | Mongall |
| 8c90aa0a521992d57035f00d3fbdfd0fa7067574 | Mongall |
| 5e32a5a5ca270f69a3bf4e7dd3889b0d10d90ec2 | Mongall |
| 0db3626a8800d421c8b16298916a7655a73460de | Mongall |
| 01751ea8ac4963e40c42acfa465936cbe3eed6c2 | Mongall |

| SHA1 | Malware |
|---|---|
| 6b3032252b1f883cbe817fd846181f596260935b | Dropper |
| 741168d01e7ea8a2079ee108c32893da7662bb63 | Dropper |
| b9cc2f913c4d2d9a602f2c05594af0148ab1fb03 | Dropper |
| c7e6f7131eb71d2f0e7120b11abfaa3a50e2b19e | Dropper |
| ae0fdf2ab73e06c0cd04cf79b9c5a9283815bacb | Dropper |
| 67f2cd4f1a60e1b940494812cdf38cd7c0290050 | Dropper |
| aca99cfd074ed79c13f6349bd016d5b65e73c324 | Dropper |
| ba7142e016d0e5920249f2e6d0f92c4fadfc7244 | Dropper |
| 98a907b18095672f92407d92bfd600d9a0037f93 | Dropper |
| afaffef28d8b6983ada574a4319d16c688c2cb38 | Dropper |
| 98e2afed718649a38d9daf10ac792415081191fe | Dropper |
| bc32e66a6346907f4417dc4a81d569368594f4ae | Dropper |
| 8d569ac92f1ca8437397765d351302c75c20525b | Document exploit |
| 5c32a4e4c3d69a95e00a981a67f5ae36c7aae05e | Document exploit |
| d807a2c01686132f5f1c359c30c9c5a7ab4d31c2 | Document exploit |
| 155db617c6cf661507c24df2d248645427de492c | Modified Heyoka |
| 7e6870a527ffb5235ee2b4235cd8e74eb0f69d0e | Modified Heyoka |
| 2f0ea0a0a2ffe204ec78a0bdf1f5dee372ec4d42 | DLL-test |
| 041d9b089a9c8408c99073c9953ab59bd3447878 | DLL-test |
| 1edada1bb87b35458d7e059b5ca78c70cd64fd3f | DLL-test |
| 4033c313497c898001a9f06a35318bb8ed621dfb | DLL-test |
| 683a3e0d464c7dcbe5f959f8fd82d738f4039b38 | DLL-test |

| SHA1 | Malware |
| --- | --- |
| 97d30b904e7b521a9b7a629fdd1e0ae8a5bf8238 | DLL-test |
| 53525da91e87326cea124955cbc075f8e8f3276b | DLL-test |
| 73ac8512035536ffa2531ee9580ef21085511dc5 | DLL-test |
| 28b8843e3e2a385da312fd937752cd5b529f9483 | Installer |
| cd59c14d46daaf874dc720be140129d94ee68e39 | Upan component |

**IP Addresses:**

| C2 IPs | Malware |
|---|---|
| 10[.]100[.]0[.]34 (Internal IPs) | Mongall |
| 10[.]100[.]27[.]4 (Internal IPs) | Mongall |
| 172[.]111[.]192[.]233 | Mongall |
| 59[.]188[.]234[.]233 | Mongall |
| 64[.]27[.]4[.]157 | Mongall |
| 64[.]27[.]4[.]19 | Mongall |
| 67[.]210[.]114[.]99 | Mongall |

| C2 IPs | Malware |
|---|---|
| 45[.]77[.]11[.]148 | Heyoka |

## C2 Domains:

| C2 Domain | Malware |
|---|---|
| back[.]satunusa[.]org | Mongall |
| baomoi[.]vnptnet[.]info | Mongall |
| bbw[.]fushing[.]org | Mongall |
| bca[.]zdungk[.]com | Mongall |
| bkav[.]manlish[.]net | Mongall |
| bkav[.]welikejack[.]com | Mongall |
| bkavonline[.]vnptnet[.]info | Mongall |
| bush2015[.]net | Mongall |
| cl[.]weststations[.]com | Mongall |
| cloundvietnam[.]com | Mongall |
| cpt[.]vnptnet[.]inf | Mongall |
| dns[.]lioncity[.]top | Mongall |
| dns[.]satunusa[.]org | Mongall |
| dns[.]zdungk[.]com | Mongall |
| ds[.]vdcvn[.]com | Mongall |
| ds[.]xrayccc[.]top | Mongall |
| facebookmap[.]top | Mongall |
| fbcl2[.]adsoft[.]name | Mongall |
| fbcl2[.]softad[.]net | Mongall |
| flower2[.]yyppmm[.]com | Mongall |
| game[.]vietnamflash[.]com | Mongall |

**C2 Domains:**

| C2 Domain | Malware |
|---|---|
| hello[.]bluesky1234[.]com | Mongall |
| ipad[.]vnptnet[.]info | Mongall |
| ks[.]manlish[.]net | Mongall |
| lepad[.]fushing[.]org | Mongall |
| lllyyy[.]adsoft[.]name | Mongall |
| lucky[.]manlish[.]net | Mongall |
| ma550[.]adsoft[.]name | Mongall |
| ma550[.]softad[.]net | Mongall |
| mail[.]comnnet[.]net | Mongall |
| mail[.]tiger1234[.]com | Mongall |
| mail[.]vdcvn[.]com | Mongall |
| mass[.]longvn[.]net | Mongall |
| mcafee[.]bluesky1234[.]com | Mongall |
| media[.]vietnamflash[.]com | Mongall |
| mil[.]dungk[.]com | Mongall |
| mil[.]zdungk[.]com | Mongall |
| mmchj2[.]telorg[.]net | Mongall |
| mmslsh[.]tiger1234[.]com | Mongall |
| mobile[.]vdcvn[.]com | Mongall |

**C2 Domains:**

| C2 Domain | Malware |
|---|---|
| moit[.]longvn[.]net | Mongall |
| movie[.]vdcvn[.]com | Mongall |
| news[.]philstar2[.]com | Mongall |
| news[.]welikejack[.]com | Mongall |
| npt[.]vnptnet[.]info | Mongall |
| ns[.]fushing[.]org | Mongall |
| nycl[.]neverdropd[.]com | Mongall |
| phcl[.]followag[.]org | Mongall |
| phcl[.]neverdropd[.]com | Mongall |
| pna[.]adsoft[.]name | Mongall |
| pnavy3[.]neverdropd[.]com | Mongall |
| sky[.]bush2015[.]net | Mongall |
| sky[.]vietnamflash[.]com | Mongall |
| tcv[.]tiger1234[.]com | Mongall |
| telecom[.]longvn[.]net | Mongall |
| telecom[.]manlish[.]net | Mongall |
| th-y3[.]adsoft[.]name | Mongall |
| th550[.]adsoft[.]name | Mongall |
| th550[.]softad[.]net | Mongall |
| three[.]welikejack[.]com | Mongall |
| thy3[.]softad[.]net | Mongall |

**C2 Domains:**

| C2 Domain | Malware |
|---|---|
| vdcvn[.]com | Mongall |
| video[.]philstar2[.]com | Mongall |
| viet[.]vnptnet[.]info | Mongall |
| viet[.]zdungk[.]com | Mongall |
| vietnam[.]vnptnet[.]info | Mongall |
| vietnamflash[.]com | Mongall |
| vnet[.]fushing[.]org | Mongall |
| vnn[.]bush2015[.]net | Mongall |
| vnn[.]phung123[.]com | Mongall |
| webmail[.]philstar2[.]com | Mongall |
| www[.]bush2015[.]net | Mongall |
| yok[.]fushing[.]org | Mongall |
| yote[.]dellyou[.]com | Mongall |
| zing[.]vietnamflash[.]com | Mongall |
| zingme[.]dungk[.]com | Mongall |
| zingme[.]longvn[.]net | Mongall |
| zw[.]dinhk[.]net | Mongall |
| zw[.]phung123[.]com | Mongall |

| C2 Domain | Malware |
| --- | --- |
| cvb[.]hotcup[.]pw | Heyoka |
| dns[.]foodforthought1[.]com | Heyoka |
| test[.]facebookmap[.]top | Heyoka |

## Appendix 1C –ToddyCat

| Ninja C2 |
| --- |
| 149.28.28[.]159 |
| eohsdnsaaojrhnqo.windowshost[.]us |

| Hashes |
| --- |
| 5cfdb7340316abc5586448842c52aabc |
| 93c186c33e4bbe2abdcc6dfea86fbbff |
| 5a912beec77d465fc2a27f0ce9b4052b |
| f595edf293af9b5b83c5ffc2e4c0f14b |
| 5a531f237b8723396bcfd7c24885177f |
| 1ad6dccb520893b3831a9cfe94786b82 |
| f595edf293af9b5b83c5ffc2e4c0f14b |
| 8a00d23192c4441c3ee3e56acebf64b0 |
| 5e721804f556e20bf9ddeec41ccf915d |

# 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