Payatu

October 2022

Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

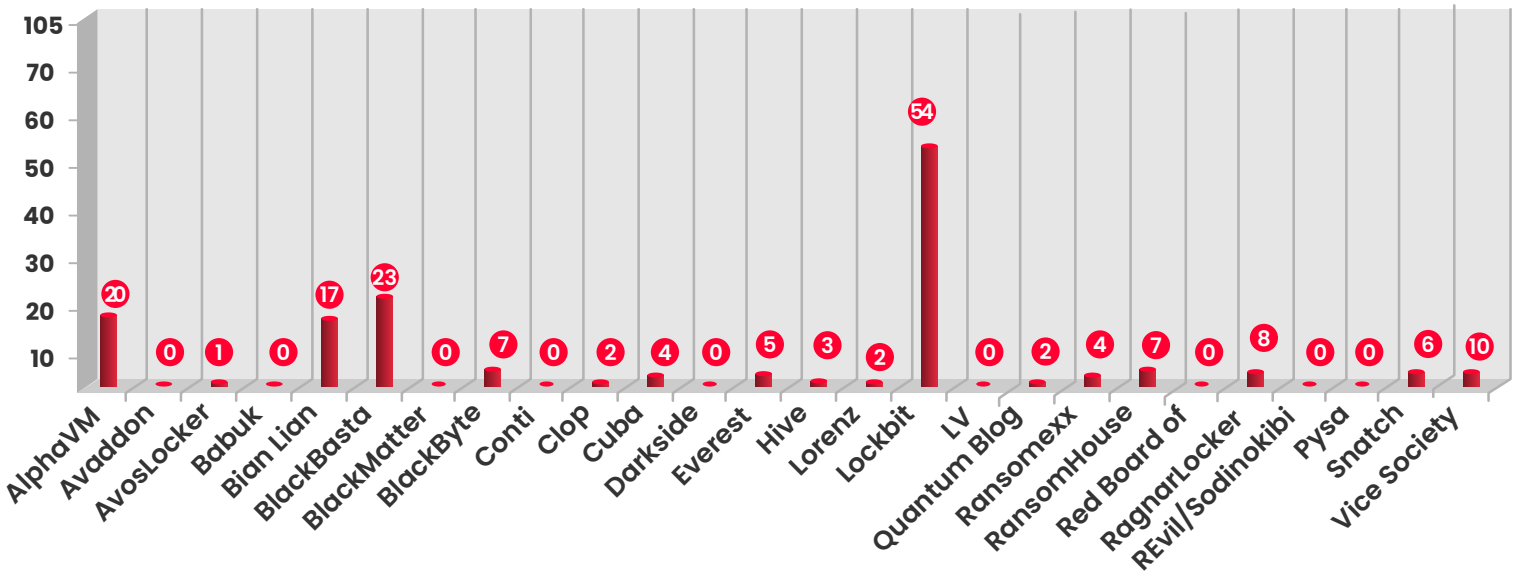
Table of Contents

01

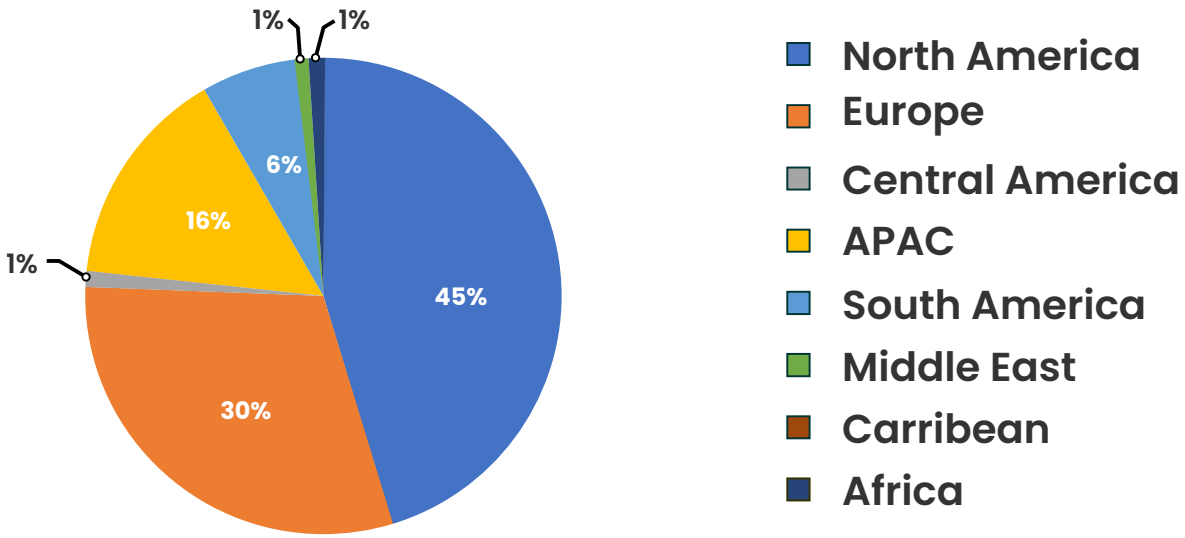
Ransomware Statistics

- Oil India Limited claimed to be compromised by Snatch Ransomware
- Ferrari claimed to be compromised by Ransomexx Ransomware, company denies it
- Tata Power compromised by Hive ransomware disclosed on October 24th
- AT&T claimed to be compromised by Everest ransomware on October 28th
- Thales group claimed to be compromised by Lockbit 3.0 disclosed on October 31st

Attacks Trend by Ransomware



Region-wise Attacks Trend



Country-wise Attacks Trend - 175

 United States - 73

 United Kingdom - 12

 France - 7

 Brazil -6

 Germany - 6

 Belgium - 5

 Spain - 5

 Canada - 4

 India - 4

 Japan - 4

 Taiwan - 4

 Thailand - 4

 Australia - 3

 Colombia - 3

 Italy - 3

 Philippines - 3

 Romania - 1

 Uruguay - 1

 Switzerland - 3

 Argentina - 2

 Austria - 2

 Greece - 2

 Mexico - 2

 New Zealand - 2

 Bahrain - 1

 China - 1

 Costa Rica - 1

 Dominican Republic - 1

 Ecuador - 1

 Greenland - 1

 Israel - 1

 Malaysia - 1

 Monaco - 1

 Poland - 1

 Portugal - 1

 Russia - 1

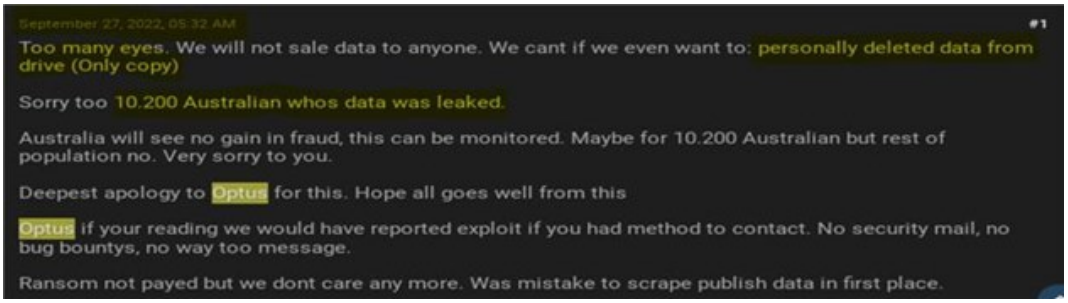
 South Africa - 1

02

After Optus, Australian Telecom Giant Telstra Corp Breached

Tags: Australia, Telecommunication, Telstra, Data Leak

Weeks after all the drama, apologies, and reeling in at the Optus data breach, the threat actor who compromised millions of customer records, published the sample data of 10,200 customers. The hacker later denied selling any data and apologized to 10,200 Australians for data leak, now Telstra Corp Ltd, another big telecom firm shared the news of a minor data breach.



Source: Breached forum(http://breached65xqh64s7xbkvqgg7bmj4nj7656hcb7x4g42x753r7zmejqd[.]onion)

Telstra, through its Twitter handle and on its exchange page disclosed details of what was happening at their network, after a buzz went around regarding a data breach in the company. Declaring that customer data was not involved in the breach, the team shared that the breach was from 2017, which happened on a third-party platform called WorkLife NAB. The breach was of a basic nature involved employee data, constituted first/last names and email addresses.

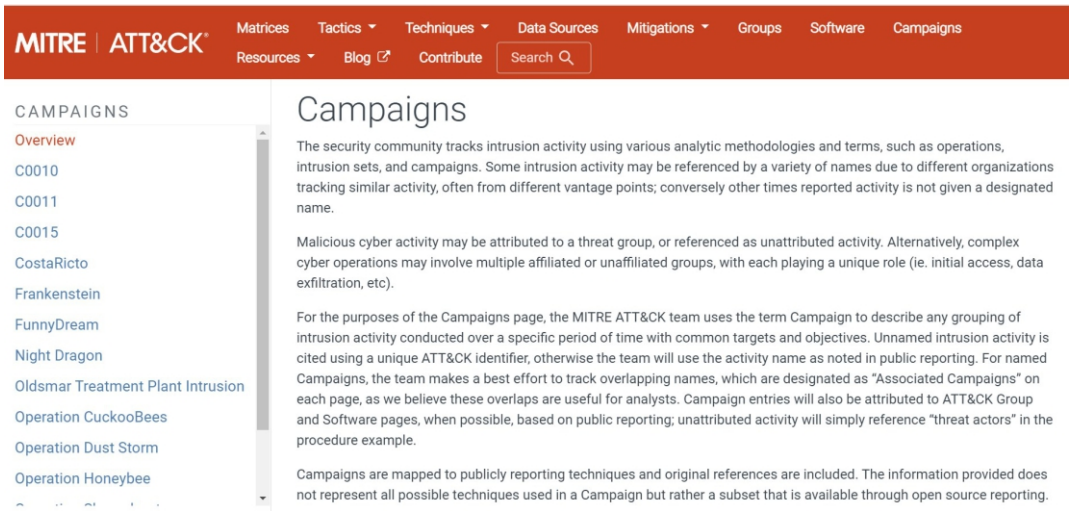
03

October 2022 Update for MITRE ATT&CK Framework Out

Tags: MITRE, ATT&CK, ICS, Campaigns

Various contributors provided their input and MITRE released its October 2022 update of the MITRE ATT&CK v12 on October 25th, 2022. The major contributions made to this update are detections to ATT&CK for ICS (Industrial Control Systems) and the introduction to Campaigns, under Enterprise section. The new addition to ATT&CK for ICS leverages host and network-based collection and ICS-specific sources such as Asset and Operational databases.

For the Enterprise matrix, the Campaign data structure is added, which contains details about various intrusion activities that have been consistent over a specific time period and the groups that have been using them. These include C0011-Transparent Tribe targeting the Indian Government, and C0015-Conti ransomware playbook.



In this release, there are 14 Tactics, 193 Techniques, 401 Sub-techniques, 135 Groups, 14 Campaigns, and 718 Software.

04

Tata Power Hit by Hive Ransomware Attack

Tags: Tata Power, India, Hive Ransomware

Tata Power, India's largest integrated power company, disclosed to BSE (Bombay Stock Exchange) Limited and NSE (National Stock Exchange) Limited on October 14th, 2022, that it was hit by a cyber-attack on its IT infrastructure impacting some of its IT systems. The company also confirmed in its letter that all its critical operational systems were functioning. While the responsible behavior of the company gained praise from the cybersecurity experts in India, no further details about the attack were shared. However, on eve of October 24th, 2022, Hive ransomware group uploaded details of their new victim which was Tata Power.

Hive ransomware group, which has been operative since mid 2021, uploaded details on their hiveleaks darkweb link, which claimed to have compromised Tata Power on October 3rd, 2022, releasing employee-related data (email addresses, passports, phone numbers, taxpayers' information, etc.) some signed documents, NDA agreements, and some other documents.

14th October 2022
BJ/SH-L2N/

BSE Limited
Corporate Relationship Department
1st Floor, New Trading Ring,
Rotunda Bldg., P. J. Towers,
Dalal Street, Fort,
Mumbai 400 001.
Scrip Code: 500400

National Stock Exchange of India Limited
Exchange Plaza,
Bandra Kurla Complex
Bandra East
Mumbai – 400 051
Scrip Code: TATAPOWER EQ

Dear Sirs,

Cyber attack

The Tata Power Company Limited had a cyber attack on its IT infrastructure impacting some of its IT systems.

The Company has taken steps to retrieve and restore the systems. All critical operational systems are functioning; however, as a measure of abundant precaution, restricted access and preventive checks have been put in place for employee and customer facing portals and touch points.

The Company will update on the matter going forward.

Yours faithfully,
For The Tata Power Company Limited

HANOZ MINOO MISTRY
Digitally signed by HANOZ MINOO MISTRY
Date: 2022.10.14 18:56:57 +05'30'

H. M. Mistry
Company Secretary

Source: NSE archive

Source: HiveLeaks website (hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd[.]onion)

05

Ransomexx Posts Leaked Data of Ferrari, Manufacturer Denies the Claim

Tags: Ransomexx, Ferrari, Italy

Ferrari, the renowned manufacturing company famous for its luxury cars, was in the news this month for a slightly different scenario. Claiming to have hacked Ferrari, was a ransomware named Ransomexx. Ransomexx, which has been operational since 2018, came into limelight after various attacks in mid 2020. The ransomware is affiliated with a financially motivated cybercriminal group, named GOLD DUPONT (aka SPRITE SPIDER) and uses stolen credentials to gain remote access services like Virtual Desktop Infrastructure (VDI) and Virtual Private Network (VPN), Trickbot malware, and IcedID as an initial access vector.

The attacker shared the files on their Data-leak-site (DLS) that constituted fourteen 500 MB zip folders and one 158 MB folder, which allegedly contained some internal documents, data sheets, repair manuals, etc.

Source: Ransomexxx blog (rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad[.]onion)

However, the Italian luxury car maker denied all claims of a data breach at its end, suggesting no evidence of a breach or ransomware attack on its systems or disruptions of any kind.

For detailed information, refer to The Records' official website

06

Intel Confirms Source Code Leak for Alder Lake BIOS

Tags: Intel, Alder Lake, Source code, BIOS

On October 8th, 2022, an unknown individual posted the source code of Intel's Alder Lake BIOS that was released on November 4th, 2021. The source code leaked on 4chan, is compressed to the size of 2.8 GB and was also available on GitHub for a while before being removed. Containing multiple files and tools for building a BIOS/UEFI for Intel platforms and chipsets, the git log contained a possible source from where this source code was leaked, speculating it to be LCFC, a Lenovo group venture.

As confirmed by an Intel spokesperson to one of the media outlets, the source code was leaked by one of its third parties, and though the leak may have occurred, it did not add up to any security vulnerabilities. There are a few keys available in the leak, and secrets such as MSRs (Model Specific Registers reserved for privileged code)that may lead to security issues. Though the immediate threat from this code leak might not appear big, in the long run, it is highly possible that the rigorous analysis of the code may result in discovery of vulnerabilities, like those used in the NSA exploits such as EternalBlue, vulnerabilities like Meltdown and Spectre.

07

Binance Hacked, 2 Million BNB Withdrawn

Tags: Binance, Cryptocurrency, BNB

After a massive attack, cryptocurrency exchange Binance suspended its blockchain network for some time. The attack resulted in a major loss of $570 million worth of BNB tokens to the hackers. The hackers used an exploit that affected its native cross-chain bridge known as BSC Token Hub, linking BNB Beacon Chain and BNB Smart Chain. The native cross-chain bridge is a type of decentralized application using tokens for locking/unlocking chains through smart contracts at the source and destinations.

Withdrawing a total of 2 million BNB, the hackers had exploited a common library used in cross-chain bridges, allowing them to send the money to their crypto wallets. The company now suggests bringing about a new on-chain governance mechanism that will help them fight and defend against possible attacks in the future. The business impact of this attack on BNB was heavy, as BNB sank more than 3 percent on various crypto exchanges. The Cross-chain bridging is known to have been used previously as well for targeting crypto exchanges due to unresolved issues in its design and because it acts as a central storage point for funds.

08

Chinese APT Group Targeting IT and Telecommunication Service

Tags: China, Asia, IT, Telecommunication

Researchers at Sentinel One have been monitoring a new Chinese threat actor, codenamed WIP19, who has been targeting IT and telecommunication service providers in the Middle East and Asia, using a stolen digital certificate issued by a company "DEEPSoft". Active since 2014 the threat actor has similarities with activities of Operation Shadow Force, using different techniques and malware.

Understanding the technical details of different malware the group uses, we see backdoors like WinEggDrop which gives remote administration ability through a custom server on an attacked machine, related DLL files consist of tback.dll. Another malware that has been identified as part of WIP19's arsenal is **SQLMaggie**, which has affected servers in more than 40 countries, geographically focusing on South and Southeast Asia. The attack is an extended stored procedure DLL used to interact outside the SQL server. Redirecting ports and performing network bridge functions are a few of the abilities of this malware. It is interesting to know that both these malwares overlap in activities of ShadowForce and WIP19.

09

APT Group Targeting Pakistan Government Agencies via New Backdoor

Tags: Sidewinder, Pakistan, Backdoor, Warhawk

Sidewinder APT, aka T-APT4 and RattleSnake, is a suspected Indian TAG (Threat Actor Group) that has been known for targeting military establishments, government institutions, and business organizations throughout Asia, with a focus on Pakistan. Active since 2012, the group has now been observed by researchers at Zscaler for targeting Pakistan through campaigns using a new backdoor, named "WarHawk" by the researchers.

The malware consists of four modules for downloading, executing, exfiltrating and uploading the exfiltrated data to C2. WarHawk downloads a Cobalt Strike payload, which executes process injection, along with a time zone check set to Pakistan Standard Time, in order to execute the loader only in those time zone machines. This downloads an ISO file along with pdf files hosted on Pakistan's National Electric Power Regulatory Authority's website. These files and malware have been observed actively this year for performing espionage activities.

10

Russian Hacker Arrested for Allegedly Hacking the JEE Mains Hosting Software

Tags: India, Government, Russia

Central Bureau of Investigation (CBI) India, shared a press release on October 3rd, 2022, updating people about an ongoing case of cyber fraud related to the Joint Entrance Exams (JEE) 2021. Under allegations of irregularities during the exam, directors, employees, and a few associates of a private education institution were arrested for attempting to manipulate the online software used for conducting JEE Mains exam and taking remote access to the systems to solve the questions for aspirants.

Bureau of Immigration at IGI airport arrested a Russian nationalist while he was arriving in India from Kazakhstan. The Russian national allegedly compromised the iLeon software used for conducting exams by adding a remote access capability to the systems of aspirants who would in return pay the institution and the hacker for an easy access into NITs and other colleges. Conducting raids last year, a total of 25 Laptops, 7 PCs, 30 post-dated cheques, and various student related documents were recovered from 19 different places in India. The attack is a clear indication that cyber threats and frauds are not just eminent in sectors like IT, Government, Finance, but awareness also needs to be spread for attacks in such unconventional sectors.

11

Google Initiates New Community Project to Safeguard Against Supply Chain Attacks

Tags: Google, Open source, Supply Chain Attacks

In the wake of increased supply chain attacks of Log4j level severity, Google is starting a new open source project called GUAC (Graph for Understanding Artifact Composition). GUAC is collaborating with various groups providing access to Software Bill Of Material (SBOM) tools, SLSA tools, and most importantly vulnerability databases that aggregate information across multiple sources.

GUAC aggregates software security metadata into graph databases, which can be queried to assist organizations in audit, policy and risk management. It focuses on four major functionalities: Collection, Ingestion, Collation, and Query. The queries to these databases can be used to identify critical libraries that can be exploited and to provide ways to mitigate such issues.

12

Appendix

Appendix 1A- Hive ransomware

Hashes
fd3e7d0f6a31b821604707ef99da281e4fd7d11c7804e46eeed11f66b200a391
321dOc4f1bbb44c53cd02186107a18b7a44c840a9a5fOa78bdac06868136b72c
be1565961e123f52e54e350eOca2666f8ffa42fdc46df18dca6f7cOac2b43d23
3ec89b737c5b91eb9daoa2d9c6c1foe637087b4552e26806d959c11f8f06e96f
le21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07dbOff
fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf
c04509c1b80c129a7486119436c9ada5b0505358e97c1508b2cfb5c2a177ed11
88f7544a29a2ceb175a135d9fa221cbfd3e8c71f32dd6b09399717f85ea9afd1
aOb4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749
5954558d43884da2c7902ddf89cOcf7cd5bf162d6feefe5ce7d15b16767a27e5
77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc661
612e5ffd09ca30ca9488d802594efb5d41c360f7a439df4ae09b14bce45575ec
a290ce75c6c6b37af077b72dc9c2c347a2eede4fafa6551387fa8469539409c7
977b2ce598bd6518913fe216d1139c041e159a6510cd71a6a14a49570c1019be
e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173
d1aa0ceb01cca76a88f9ee0c5817d24e7a15ad40768430373ae3009a619e2691

Hashes
8f3c5f9cd657e3785d751305023cf83a7f27780d5441817614d442e28dbe3ac4
c367ab50c1f103963da0f0404eeda46c9e768711797d638afa1c4cf740575613
fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf
ed614cba30f26f90815c28e189340843fab0fe7ebe71bb9b4a3cb7c78ff8e3d2
1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff
fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf
c04509c1b80c129a7486119436c9ada5b0505358e97c1508b2cfb5c2a177ed11
a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749
5954558d43884da2c7902ddf89c0cf7cd5bf162d6feefe5ce7d15b16767a27e5
77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc661
e514be3e997895c7e3ece03549c8cb6b5700fe8f814948ed201ca59daa8733fb
7b7f13ab85bc78849e04a5589c84f0ec1847460106c03ca3db84703c7af054f3
bdf3d5f4f1b7c90dfc526340e917da9e188f04238e772049b2a97b4f88f711e3
6983ef6e484c0c70356d6f868ac03bc90a1055560642706743511f76aa6f28ad
6a0449a0b92dc1b17da219492487de824e86a25284f21e6e3af056fe3f4c4ec0
5d95bf2518918422a6cac03f90548f02a5848dbc43836868636b61d0a87ed968
47006ed84afb1f1fd761b81f3ae7b6547c0cb4845538301035e1388693fc6f7f
25793a0764a51b38806b7dcf5f5d8df9620f090f72362aa03187c8813e054482
7b7f13ab85bc78849e04a5589c84f0ec1847460106c03ca3db84703c7af054f3
5d95bf2518918422a6cac03f90548f02a5848dbc43836868636b61d0a87ed968
d64f9742539436acba5ff9c4f1c8ca501cad86dfa823828b65418b493c8109ac
5d95bf2518918422a6cac03f90548f02a5848dbc43836868636b61d0a87ed968

Hashes
bd6d8f7c9e016dd7395ee7f0f8485de622a9b034b7c5d2e1af25cb762dd8d8c9
0e8e6fc94e6eb17cfd8993b3dcfd9acd11ee32f1b4e956df3097ae3259be4f9c
875708f911752bef7e2ef0658d395ebeccef774d5fdb74f6e9ee60b52d86cbf0
5b32ac4754bd5728cc7a68f341bf64cec4a737eb584814bb2099a5f2ff69e584
baa7a6e5a093ee6be47eca86e5acbcba196c7d1d35662eecad23ec870702116a
a2ad0442cebe3e6abb86069a3b66b471b4a7c9d00286da4b8114d17a849128d6
321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a78bdac06868136b72c
6bd3adc7e43e20ede1a82ad1469cc7ecd085b324621edbd4ec23db4e4473895f

Appendix 1B- Ransomexx

SHA256
f543c477ba67afd4fb2ae111b22c8d596bf8e61e13a627f6a972fac4762a70c1
ed2b1f855fc7a39a7cf2cfbfd5a10707801ba313bab9c5d748fcd3703aad66fc
e55fcf9315c52d2abd3431f7e4bb82cbd2b0d24d124e0e1a27b951030b2de162
d85f4448d5aea240d68c07bec6f363986d71940c3c1a3e49053d55fd1741c41e
d1429f54baaad423a8596140a3f70f7d9f762373ad625bda730051929463847d
cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849
8d2b3b0cbb32618b86ec362acd142177f5890917ae384cb58bd64f61255e9c7f
78147d3be7dc8cf7f631de59ab7797679aba167f82655bcae2c1b70f1fafc13d
64c51351aafb4cd339934a78d064847bdd833b963eafbade86eb51ac2c1677f4
5f2f33a47904d1882455c431f327b326926afac8064b2eccba59fb037b95b0d3
4cae449450c07b7aa74314173c7b00d409eabfe22b86859f3b3acedd66010458
01e8cf9c1390dfe2b486e7bdd12f01aeb634fbf4d88890435ee97da401810049
01e8cf9c1390dfe2b486e7bdd12f01aeb634fbf4d88890435ee97da401810049

SHA1
e7748b92347f95589fa739cbe5c089046614ce92
d2716833296317323f7cce5691940ab0b58e36d7
91ad089f5259845141dfb10145271553aa711a2b
6b5e5a742a8b98b9a87cf317ff694797d49d756a
6a0a7e3a21888b87fde3323e0dc4fc085e71a8b7

SHA1
58c581a7f819cf326cadc3db4f43ffcd8203ee5e
5448e52acc4bfe16cebaef661ca19a913e189bd4
50f191f04aa6cff1d8688a3c5d6cce96739ab6b3
3555aaebe6c113fb8f923a38cb3bd75da6e86277
33e792ebbd5b4b75b84de2ddf4d47599339f2896
30391fe6c4ba0b13050863089249c5a7c8f162e2
1bc3dce31fe1beb727cd449e6cec70578c5dcb55
142b147c3b5597dead28d8ba91927ac0a960bf41
0abaa05da2a05977e0baf68838cff1712f1789e0
08574581b59387626aed58a824f3d84b2ea225c9
035c138f3e73b402a48c94e2d97491931b1a0038

MD5
fe571f22a4d0745a2028e52960ffbaf3
fcd21c6fca3b9378961aa1865bee7ecb
f71e0a02205b6e6b7ed5a35ada232c8e
fe571f22a4d0745a2028e52960ffbaf3
fcd21c6fca3b9378961aa1865bee7ecb
f71e0a02205b6e6b7ed5a35ada232c8e
e87bb48fe2765fabb695002f20b11876
e87bb48fe2765fabb695002f20b110a5

MD5
e87bb48fe2765fabb695002f20b10873
e57c25f7969f03dc47ec6ea04d2fe9d9
e4c99cd6346d2f1d97b328c2071a4e12
e4c99cd6346d2f1d97b328c20713b3ab
e4c99cd6346d2f1d97b328c20713a4c3
e494c1420a2e1bf2f96ee7698f87d468
dc3f84359f2ade578eddff076f621792
d512a5abf0854e5c7657554b4ea48275
d2265abffd6f3093177d7751cef85362
cf73aa73404a5c9cf0ec50fdd0d7e9ce
ce1c01137e51ae2d0caf3a4a44319bf0
ca2326886fa699068c44f32b3e51adaf
b8b4eecdf140e57dad6d2071e6a82852
b5486edc903eda5b506e7347487477c2
b42eb225aa70bd4101c03e2ea4208adc
b2bc74d95c8bd5b5db9c02df6a6ae2d3
b1ddb9eb6ecca93c771d7232f75d12f5
aa1ddf0c8312349be614ff43e80a262f
a9686117e2f7634c819106e84a016691
a9686117e2f7634c819106e84a003e54
a8abb3ccbb0a97b127cc27fbf5d06e06

MD5
a4f33d89f8d0b0a2607065edbf91fb9f
8f3dacc0bcb80a9a29cc5cd6483492d0
8f3dacc0bcb80a9a29cc5cd6482a1202
8e5375a9f1e45cd2200d6f3e2c093314
8e5375a9f1e45cd2200d6f3e2c091532
7ee46373a0a370ee9657aebc9ef5448a
7760f56ff3c593a832f5e59db63209d5
6fc225927e1830f7c5e692197e4b98aa
6aed05c3955eda9d99cec05910be8b29
63e751462c47f95c89ab83df8d89a36a
5f94faa27dd26b1be8d62fff816e1871
5f94faa27dd26b1be8d62fff816e0d62
5a05d348be020d55bf69f109130bb283
5a05d348be020d55bf69f109130baa2d
570dc2c306b14f24b2cb160557ff4b01
56a87d00f5a18987e02433b0f42a95b3
4f0374da16a4469b553a92cb89a26836
437e30fdb138801e17543edd395a783b
2b0ae63aa23b37abd6e51c5954d1be21
21cac236ae439548546d5ac92b83c5e5
210f47c8f47ded8525da927710abc6ad

MD5
1a546d8713bffdef3aa74b7f01f3a25e
129a057445edf42315c6d626c85dba3b
129a057445edf42315c6d626c852fd2f
129a057445edf42315c6d626c852f9af
09984d531d55abce0bd1357f87e93b9c

Appendix 1C- WIP19

SQLMaggie SHA1	Real File Name
4AABB34B447758A2C676D8AD49338C9E0F74A330	sqlmaggieAntivirus_32.dll
4AABB34B447758A2C676D8AD49338C9E0F74A330	sqlmaggieAntivirus_32.dll
5796068CFD79FBA65394114BA0EDC8CC93EAE151	sqlmaggieVS2008new_64.dll
13BA1CFD66197B69A0519686C23BDEF17955C52E	sqlmaggieVS2008new_32.dll
CA25FCBA11B3B42D9E637132B5753C9B708BE6F0	sqlmaggieVS2008new_64.dll
26cbd3588b10cabc7c63492c82808104829e9ac0	sqlmaggieAntiVirus_64.dll
5e0291928e29db46386fd0bd85f269e967758897	sqlmaggieVS2008new_64.dll
96099015981559237a52a7d50a07143870728fd0	sqlmaggieAntiVirus_64.dll
7eb6e7d4e5bd5a34c602879cad0a26b35a3ca4fb	sqlmaggieVS2008new_32.dll
fe2e7c663913e0744822d1469be0c3655d24178d	sqlmaggieAntivirus_32.dll
b15bae6a8379a951582fc7767fa8490722af6762	sqlmaggieAntiVirus_64.dll
c81de9a27f7e8890d30bd9f7ec0f705029b74170	sql_epX64_MD.dll
829df7b229220c56eedc5660e8f0e7f366fa271f	sqlmaggieAntivirus_32.dll
d02fce5d87ea1fe9fabe7ac52cae2439e8215121	sqlmaggieAntivirus_32.dll

SQLMaggie SHA1	Real File Name
1c6d0e8920af9139a8a9fe3d60b15cf01fb85461	sqlmaggieAntiVirus_64.dll
2cad0328863cb09a6b27414d5158075d69bfb387	sqlmaggieAntiVirus_64.dll
26c0722a1d16641d85b97594deea2a65399daef7	sqlbackupAntiVirus_64.dll
17ff9fc9ee72baaf8d66ef9b3ab6411c47384968	sqlmaggieAntiVirus_64.dll
5be50453f6e941c5c1dd20e0ba53e9abb6d00b68	sqlmaggieVS2008new_32.dll
56d326dfe7dcb1ce7cae2cb4c13819510fc9945c	sqlmaggieAntiVirus_64.dll
253e702ff8201eec6fdf9630a39f5a8c28b132ed	xp_OAreateX64.dll
b91ab391a4e26e4ff0717cd989ad5ce7f6af235c	xp_OAreateX64.dll
4d2eb6e03be068f364e8e3f3c9645e03e1052e66	xp_OAreate.dll
b91ab391a4e26e4ff0717cd989ad5ce7f6af235c	xp_OAreateX64.dll
4d2eb6e03be068f364e8e3f3c9645e03e1052e66	xp_OAreate.dll
8941d889cb199a234d99c90ce78a96411b6dedb6	sqlmaggieAntivirus_32.dll
5aa9a9299865b0cb81fcad5f42424d79c67c403b	sqlmaggieVS2008new_64.dll
5182e0a5f075317171ad0e01e52d32937ec2fa01	sqlmaggieVS2008new_64.dll
bfccf57e173b8233d35928956022bae85fc5d722	sqlmaggieAntiVirus_64.dll

SQLMaggie SHA1	Real File Name
18d3ac848955295381f769b923a86871e01bfa1c	sqlmaggieVS2008new_64.dll
2bf1b6163af5685824c2d7ecda4f3f65f3ca4723	sqlmaggieAntiVirus_64.dll
9577a2c15494edc2f7f4a59ecfb3ee90dd1df9d7	sqlmaggieAntiVirus_64.dll
32e96ef4754c8f357e2366078387750e7f6add43	sqlmaggieAntiVirus_64.dll
11678237dfccc88f257acca2b66b578713deaca8	sqlmaggieVS2008new_64.dll
327bedce44160ebccc7d465c673d3464e23292b9	sqlmaggieVS2008new_32.dll
7d58e51aee7da91dc93025854712cee47ed03101	sqldoorVS2005_64.dll
4a6cf3d5b005e97ef6f2be09f8ab19c2755cae39	sqlmaggieAntiVirus_64.dll
f37d9ce547894ab5449e5632188a3a3bb9e91fed	sqlbackupAntiVirus_64.dll
a347aaf152d8ddcd299d86d7839d4ffa369ef2ef	sqlmaggieVS2008new_32.dll
f2c64108cb670e82908e5f41c58f1aab97ee7786	sqlmaggieVS2008new_64.dll
a34bda87bd253eda794462c20074baed19e1c01c	sqlmaggieAntiVirus_64.dll
df1a7c13a3ec612a10819353ba0d34348a404bc8	sqlmaggieAntiVirus_64.dll
b3249b6f05eeeb2cf5f74931aa990fbc92027b54	sqlmaggieAntiVirus_64.dll
d3eeb9db89f0b21dc945f5410be9a9532e0c951e	sqlmaggieAntiVirus_64.dll

ScreenCap SHA1	Real File Name
c6cb7ec82ee55ccb56a4cc8b91c64e9b4f4e14da	ScreenCapDll_x64.dll
19f2a546a76458dda6eab6e2fae07d0942759b84	ScreenCapDll_x64.dll
693e4ed784279bc47a013dc56f87cbd103e1db2e	x
ad72aa442ff2c357b48ae8b4f8ba9b04b63c698b	ScreenCapDll.dll

Hacking Tool SHA1	Description
da876cd6e3528f95aafb158713d3b21db5fc780b	Browser credential stealer
1121324a15e6714e4313dfa18c8b03a6da381ba1	Credential dumper loader
9bedb5810536879fae95c70a918eb90ac628953e	Network scanning tool
539d87139de6d5136b6d45dbc33a1aae69926eee	Credential dumper
afe25455804a7afb7639cb4e356cb089105be82d	Port relay tool
37cca724227a8e77671ecde3d295f5b98531705b	Credential dumper loader
2eeb46d538c486f8591a78a65dde250b0bf62f89	Windows domain tool

WindropEgg	Descriptio
13eaf5c0c0a22b09b9dead93c86f085b6c010e3413b0e27c0616896978871048	Port scanner

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