Red Piranha
unified threat management

THREAT INTELLIGENCE REPORT

Dec 31, 2024 - Jan 06, 2025

Report Summary:

- **New Threat Detection Added** – 2
  - o New Mirai Variant
  - o LandUpdate808 Fake Update Variant
- **New Threat Protections - 163**

The following threats were added to Crystal Eye XDR this week:

1. New Mirai Variant

A recent analysis has identified a new variant of the Mirai botnet, known for targeting IoT/Linux devices across various architectures, including ARM, MIPS, and x86. This variant, referred to as Mirai.CatDDoS or GorillaBot, is operated by the CatDDoS group and incorporates the TEA algorithm for encryption, deviating from the original Mirai's XOR-based string decryption. Notably, it lacks the Telnet brute force scanning module present in the original Mirai, focusing instead on enhanced DDoS attack capabilities. The malware communicates with its command-and-control (C2) servers using hardcoded OpenNIC DNS servers and employs a broader range of attack vectors compared to its predecessor.

Threats Protected: 02
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Alert	Alert
OT	Reject	Drop

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059	Command and Scripting Interpreter
Impact	T1499	Endpoint Denial of Service
Command-and-Control	T1071	Application Layer Protocol

2. LandUpdate808 Fake Update Variant

LandUpdate808 is a recently identified fake update malware variant that deceives users into downloading malicious payloads by presenting fraudulent software update prompts. Unlike other fake update malware such as SocGholish, LandUpdate808 employs a distinct delivery mechanism involving specific URI patterns like /p/land.php and /wp-content/uploads/update.php. The malware's payloads are typically named following the pattern update_DD_MM_YYYY_####### and have been observed with .js, .exe, or .msix extensions. The initial infection vector involves injecting malicious scripts into compromised websites, which then display fake update pages to visitors, prompting them to download and execute the malicious payload.

Threats Protected: 14
Rule Set Type:

Ruleset	IDS: Action	IPS: Action
Balanced	Reject	Drop
Security	Reject	Drop
WAF	Disabled	Disabled
Connectivity	Disabled	Disabled
OT	Reject	Drop

Class Type: Trojan-activity

Kill Chain:

Tactic	Technique ID	Technique Name
Initial Access	T1566.002	Spearphishing Link
Execution	T1059.001	Command and Scripting Interpreter
Defence Evasion	T1218.010	System Binary Proxy Execution: Regsvr32
Command-and-Control	T1071.001	Web Protocols

Known exploited vulnerabilities (Week 1 January 2024):

Vulnerability	CVSS	Description
CVE-2024-3393	8.7 (High)	Palo Alto Networks PAN-OS Malicious DNS Packet Vulnerability

For more information, please visit the **Red Piranha Forum**:
https://forum.redpiranha.net/t/known-exploited-vulnerabilities-catalog-1st-week-of-january-2025/535

Updated Malware Signatures (Week 1 January 2024)

Threat	Description
Lumma Stealer	A type of malware classified as an information stealer. Its primary purpose is to steal sensitive information from infected systems, including but not limited to credentials, financial information, browser data, and potentially other personal or confidential information.
Mirai	A malware that turns networked devices running out-of-date Linux-based firmware—such as routers, IP cameras, and other Internet of Things (IoT) devices—into remotely controlled bots. These bots are then used as part of a botnet in large-scale Distributed Denial of Service (DDoS) attacks.

Ransomware Report

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. In the past week, our monitoring revealed multiple ransomware incidents across diverse threat groups, underscoring the persistent and widespread nature of these cyber risks. Presented below is a detailed breakdown of ransomware group activities during this period.

Ransomware Group	Overall Percentage of total attack coverage
El Dorado	1.92%
DarkVault	3.85%
RansomHub	15.38%
RansomHouse	1.92%
RA Group	7.69%
Inc Ransom	1.92%
Space Bears	1.92%
DragonForce	3.85%
Arcus Media	13.46%
FunkSec	1.92%
Play	7.69%
Handala	1.92%
SafePay	13.46%
Cloak	5.77%
Ciphbit	1.92%
Cicada3301	1.92%
Hunters	1.92%
Lynx	1.92%
8base	9.62%

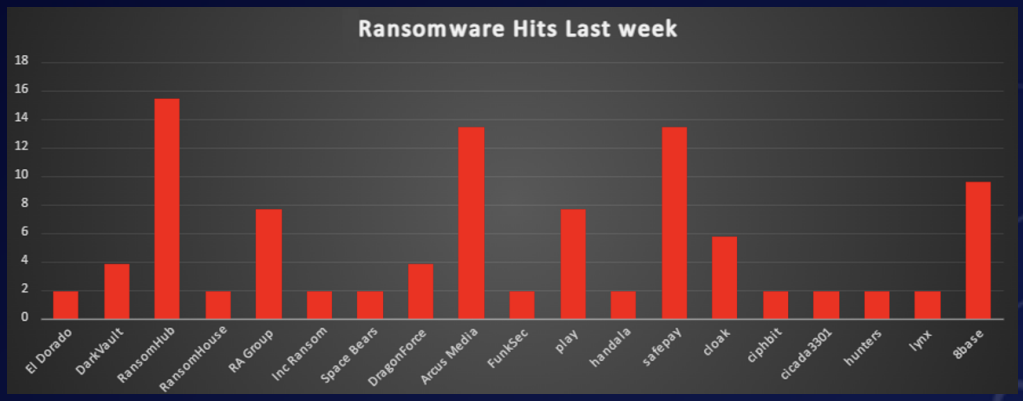


Figure 1: Ransomware Group Hits Last Week

RansomHouse Ransomware Analysis

1. Overview

The Red Piranha Team conducts ongoing surveillance of the dark web and other channels to identify global organisations impacted by ransomware attacks. Since late 2021, our monitoring has revealed consistent activity from the RansomHouse ransomware group. Despite positioning themselves as a "professional mediator community," their operations remain aggressive, combining data encryption with double-extortion tactics. They primarily target enterprise-level hypervisor systems, exploiting vulnerabilities and misconfigurations. Their attacks are supported by sophisticated tools such as Mario ESXi ransomware and the MrAgent automation tool, enabling large-scale ransomware deployments.

2. Key Findings

- Primary Targets: Corporate Windows and Linux hypervisor environments.
- Key Tools: Mario ESXi ransomware, MrAgent deployment automation tool.
- Attack Strategy: Double extortion (data encryption + public data exposure).
- Infrastructure: CDN servers, Command-and-Control (C2) servers, and Tor-based communication platforms.
- Tool Evolution: Heavy reliance on leaked Babuk ransomware source code for Mario ESXi.

3. Ransomware Tools and Techniques

3.1 MrAgent Binary

Purpose: Automates and streamlines the deployment of ransomware across extensive hypervisor environments.

Platform Compatibility: Windows & ESXi.

Key Features:

- Creates unique host identifiers using hostname and MAC addresses.
- Disables ESXi firewalls.
- Executes remote commands on infected systems.
- Removes files and drops SSH sessions.
- Modifies welcome messages displayed on ESXi hypervisor consoles.
- Maintains ongoing communication with C2 servers.

Command-and-Control Protocol: JSON-based protocol for consistent communication with C2 servers. Supports commands like info, config, exec, run, remove, abort, and quit.

Command-and-Control Protocol: JSON-based protocol for consistent communication with C2 servers. Supports commands like info, config, exec, run, remove, abort, and quit.

Windows Binary Adjustments:

- Utilises PowerShell for key functionalities.
- Limited ability to disable firewalls or modify system passwords.
- Relies on popen syscalls for command execution.

3.2 Mario ESXi Ransomware

Background: Forked from the leaked Babuk ransomware source code.

Capabilities:

- Encrypts virtual machines efficiently.
- Changes root system passwords.
- Iteratively shuts down and encrypts VMs to maximise damage.
- Blocks remote management services.

Common Commands:

- esxcli network firewall set --enabled false
- ps | grep sshd | grep -v root | awk {print "kill -9", $2} | sh

4. Tactics, Techniques, and Procedures (TTPs)

Tactic	Technique	ID	Description
Initial Access	Valid Accounts	T1078.002	Exploiting weak credentials for access
	Exploit Public-Facing Application	T1190	Vulnerabilities in public-facing systems
Resource Development	Acquire Infrastructure	T1583.004	Leveraging CDN servers for data exfiltration
Execution	Unix Shell	T1059.004	Direct execution of shell commands
Lateral Movement	Remote Services	T1021.001	Unauthorised RDP/SMB sessions
Impact	Data Encrypted for Impact	T1486	Encrypted virtual machine data
Command-and-Control	Application Layer Protocol	T1071	JSON-based communication via C2 servers
Discovery	System Network Discovery	T1016	Gathering IP and MAC address information

5. Indicators of Compromise (IOCs)

MrAgent File Hashes:

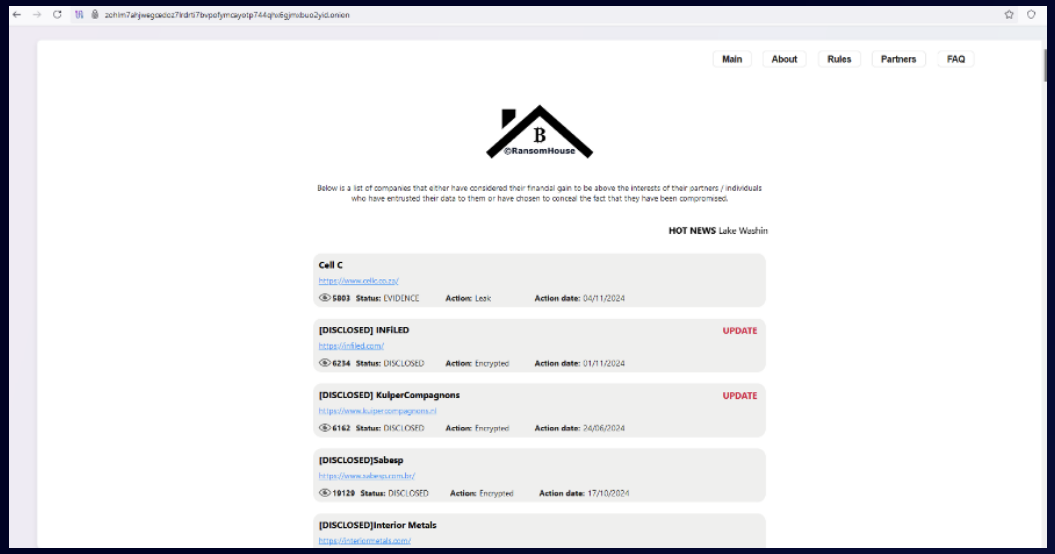
- 8189c708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973
- bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c

Mario ESXi File Hashes:

- 3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e
- afe398e95a75beb4b0508c1bbf7268e8607d03776af0b68386d1e2058b374501

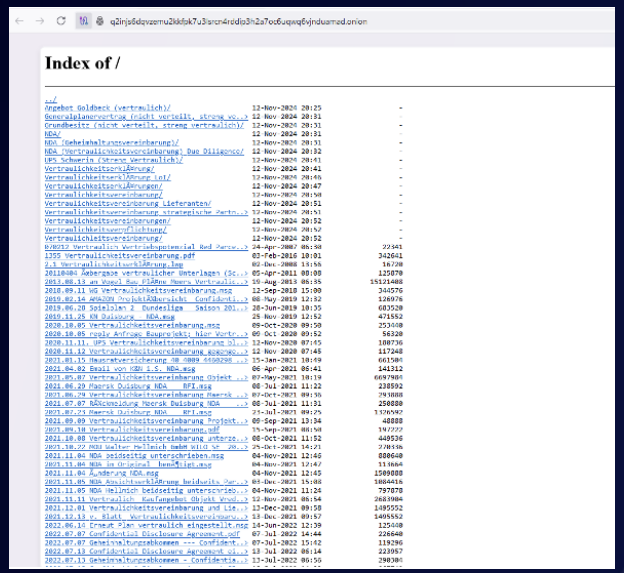
Windows-Specific Hashes:

- bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c



6. Recommendations for Mitigation
   - Patch Systems Regularly: Ensure all hypervisors are up to date.
   - Secure Remote Access: Limit access to essential services.
   - Deploy Advanced Endpoint Protection: Use EDR solutions for threat detection.
   - Backup Regularly: Store backups offline and validate integrity.
   - Monitor Traffic Patterns: Flag suspicious JSON-based C2 communications.
   - Employee Awareness: Provide regular training on phishing and social engineering.

Chat Server:



URLs
http://xw7au5pnwtl6lozbsudkmyd32n6gnqdngitjdppybudan3x3pjgpmpid.onion
http://zohlm7ahjwegcedoz7lrdrti7bvpofymcayotp744qhx6gjmxbuo2yid.onion/

File servers

http://q2injs6dqvzemu2kkfpk7u3lsrcn4rddip3h2a7oc6uqwq6vjnduamad.onion/
http://b4k2fi62ctrid4k73itusuvcz5x5yczk27bpqdrsvwu3nl5mnz5dg3id.onion/
http://gfkngfw25qwhd2sn43x7cflcehk3bb7v2uifjndr2sc3k2abhqs22rad.onion/
http://ge74uts2ybu22kzwahiayovxelbq5fwhywl73agev5w4fef2e5ikplid.onion/
http://xlirefmk3w2gsk3n5mkddinbfdatk6lhi7fj36knubhtoxiaqyus44yd.onion/
http://q2bwuip5xq4qjn2vyevprcddhk26cigyqfqfu6yki7korjys2rposaad.onion/
http://nuhnnxg3owawo36mwdffyblbzplhthfswny55mh7yhbxq74en6jihyad.onion/
http://m7vtnbsgctdcsccqmpnmi6igg3pcuiliqqqsq6uonkzg4blpa4eysiad.onion/
http://vopa354z4toilkjn4ileaf6rinkzn2givaokvj4yguq5kbiqoulxnzyd.onion/
http://helc2q6kbiyz4cwegzlp5anigkbjsbowjxrjxv3j27rjbvycgr2qd2qd.onion/
http://aw5q5nzdok52cgprlzik4n44qstoajrlbixqqukqqcennjyas4x4opad.onion/
http://bffujdbkhxfs2y63haztye4txuqgbkttmtxuxzkrlnruyioak5aoohid.onion/
http://swnoxbuqfh7dmbqzaigqllkkljspipnvft3a4offxh3m5zwxg6ob46ad.onion/
http://nw4f4x2gix7y7y3nizwj2fnf5u4tqy2mwej62r6tdqye4s5ogrtftuid.onion/
http://pnhyueueqsog3gbjuq3o7ixqbcdctpqnzv4uujsg3j76nt2bsm2p3rid.onion/
http://oujq7kjgzj4r3fyvsb2wtz6bxycrvawqdtj6zqgljw7u4hwqsak34jqd.onion/
http://jjgql4ddcs3hk5ptmfrpjriplialbjwi5a4tekffbfzv6n6oj5bmklid.onion/
http://hyinn53atxthbme4n76ry76jiaohqd6uk35jwni32g6dqtqkaejgquid.onion/
http://3nr2abdugd4mqabdmhialw3nbhol2qpywsphkocrhp6f7yxp3cps5iad.onion/
http://blofpgq5q3talt3y2w3y6r3focrtrk7ugmwl3e6a4pjuf5t2tivkxbqd.onion/
http://t7ezcjqq7h24gwswhyde72x4gkqxsjeyt2fxz44kcls6ipm4wd6bmsid.onion/
http://57yqe2tksgsmmwaqrxf45uaqy45t3hxu3dcnywjdks6lhtfztkpx57yd.onion/
http://uvl645c47e5bozdzrrtjtm6pea5oltef63tsewz5ucmubvsj5i7meiid.onion/
http://omdcwhef4ztuwhdiv3dbcgz2iyh2yb3gkkbusgvegbyjcacctahpxryd.onion/
http://uv4sykhrapb2t3mnhw6imkbdym4fh6vstwcdsvbtzrvdwzcd5zzlylqd.onion/
http://7yrwf73tckb4mtt2kms4qc7nr7rzghu3jdzycm4w4qq2nwrybi7hq7ad.onion/
http://ggyosmcjq5vw7qimqhn2bf2gbr5zhdqmrfl35nnki6q5dmvblcqsmhyd.onion/
http://rfbka2dt27wyuzymonzzx2zeaohx7sejti4gpihhc22hv74hya4h4yyd.onion/
http://lpx3qaviraf2k7uozkf2qi47beenvt4dwyr2f3zgdwjglyywhtikiead.onion/
http://oplhizp4lkdxmrydoz4ixngotsqialrexmuficduihuktq4777tlb3qd.onion/
http://kd4zqe5ao4wio7shv747uszayc2xtpvoxirs3pnm7nrld5462jzf43qd.onion/
http://cdalrbmvj36y24xbejqxgg6htzcgrbyf52ikoqgjwxvf566uycawa6id.onion/
http://agx3kdwbkrff5csgkuf7rl3uytbgraqyb5kmr2ltp7pnza4puxgsyeid.onion/
http://bqj4qln6jluwlsa32qjen2wlpgnqold4hgpkxny4x3vtsiecvdphwtqd.onion/
http://scuj56wenkc4oltbf35mxjqprwpyw7hfy4pwfwb54nfjs2ukemfodnyd.onion/
http://4bzbm2ifa2hffdb5celerb43mdbqoi6hcso3b2y4b6stdiiu2dww5bqd.onion/
http://cwiukccdpixacamo24wkdkv4pgu62xtnbfuvauvqr5zjcr4jg2w4dcyd.onion/
http://j3pbdpnbkib7evm4rhzq64vdxqd3tfgr2x25v65hfefmlukah5nfpeyd.onion/
http://mc2pt7cfb4p3xojzsmyzt2pe7chobgkbddpdqxdscks6ttbki77xl2id.onion/
http://cxkk2csneiefspqrv75vw5766sw56t67tluuekk6mm2k4f7vagh7qbyd.onion/
http://74zmq5sfydbci37dwwqd3ybkosw7wsuq5ymmc3fvyely45mtkvamh5yd.onionn/
http://uiw34f2i7x5lz2l2r33a23h3q5h3dzvrmwyz5m65uwdgkdkappn7jkyd.onion/
http://3vl65cye5nopltxxds73drcjddfq5wxwc2o5sm2rq3gddbs3ce7vn5ad.onion/
http://dj7ww4rxmvy5vsqxqn557p3nzjmt64q4fg57tteono6ezzm3nsmhgpad.onion/
http://texnb5y3cjaf2srwfjkafdzznqc3idjlncqiiobhq4yzlqw6sgvbljqd.onion/
http://otxn2ad3ypniexesajgomjnpwbkdjdit7uii2zv5v4c4u76r2rnlrtyd.onion/
http://zabhu2tvl3elihuccjzl4n35m27smgyxc5zkbgz3rcewjn6tjt2ihiad.onion/
http://vxpudlncob2ouf6pnic5khdwdb3j52ersb636c4xm3s2p2wxg6vyi4yd.onion/
http://kcikcoor63fa4qw6gx7yp2jxnvxbsxxdwd2znz72izt74rpdjfha2yqd.onion/

Ransomware Victims Worldwide

A recent ransomware analysis reveals that the United States remains the most heavily impacted nation, accounting for a staggering 38.46% of global incidents, highlighting its continued vulnerability to ransomware threats. Following this, Singapore reported 7.69% of the attacks, emerging as a notable target.

Countries including Germany, France, Spain, and Brazil each accounted for 5.77% of the incidents, reflecting a significant level of exposure. Meanwhile, Canada and Australia reported 3.85% of ransomware attacks, underscoring persistent threats across North America and Oceania.

A broader set of countries, including Mongolia, Greece, South Africa, New Zealand, Italy, Ukraine, Tanzania, India, Belgium, Vietnam, Portugal, and Japan, each contributed 1.92% to the overall ransomware incident landscape, signifying a widespread global reach of these attacks.

This analysis underscores the persistent and global nature of ransomware threats, with North America and parts of Asia bearing a significant portion of the impact. The findings emphasise the critical need for strengthened cybersecurity infrastructure, proactive defence strategies, and heightened vigilance across all sectors to combat the relentless growth of ransomware attacks worldwide.

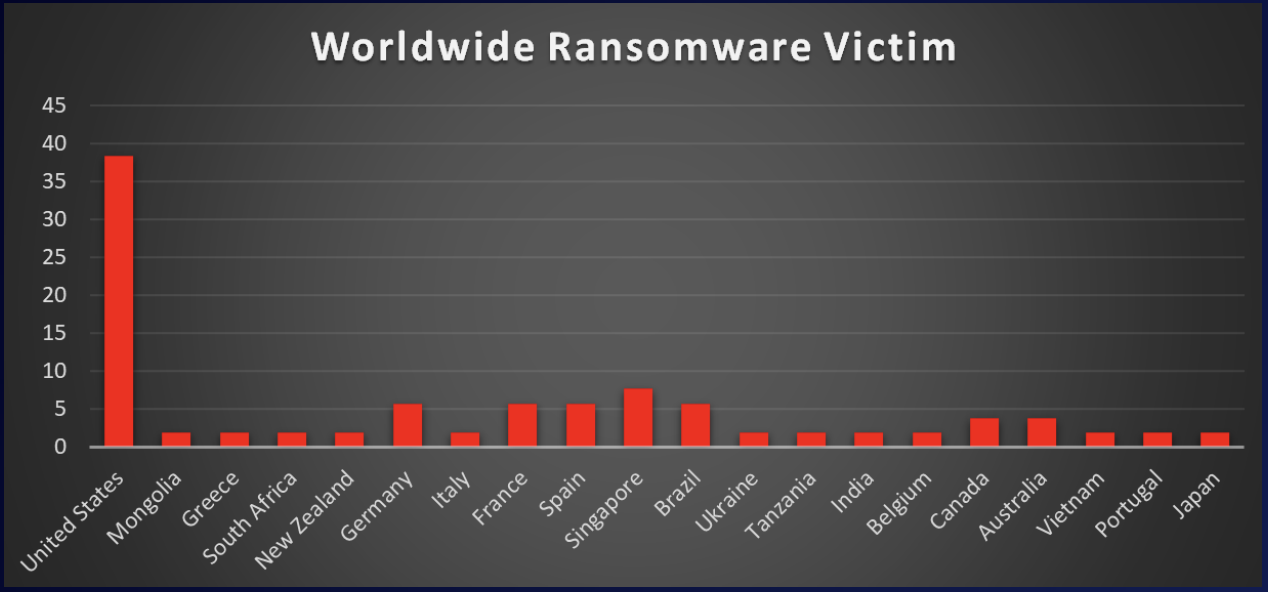


Figure 4: Ransomware Victims Worldwide

Ransomware Victims Industry-wide

A recent ransomware analysis highlights the Manufacturing sector as the most targeted industry, accounting for 19.23% of total reported incidents. This emphasises the critical vulnerability of essential production and supply chain operations to cyber threats.

Following closely are the Business Services and Construction sectors, each representing 15.38% of ransomware attacks. The Retail sector follows with 11.54%, reflecting its susceptibility due to customer-facing operations and transactional systems.

Industries such as Education (7.69%), Telecommunications, Real Estate, and Finance (each 5.77%) also faced significant ransomware exposure. Meanwhile, Healthcare and Law Firms reported 3.85% of incidents, indicating ongoing cybersecurity challenges in sectors handling sensitive data.

Sectors with a smaller, yet notable impact include Non-profit, Media & Internet, and Hospitality, each contributing 1.92% of reported incidents.

This analysis underscores the pervasive and indiscriminate nature of ransomware threats, impacting industries across critical infrastructure, public services, and commercial enterprises. The findings highlight the pressing need for tailored cybersecurity strategies, robust defences, and proactive risk management to mitigate the ever-evolving ransomware landscape effectively.

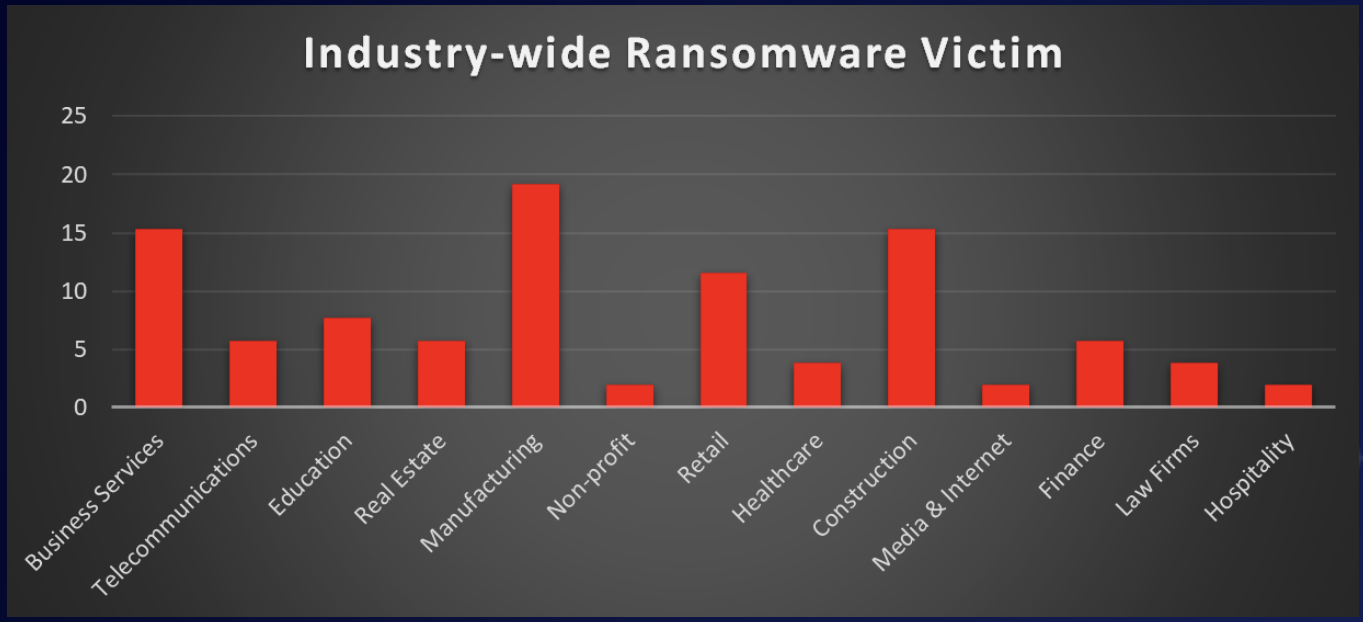


Figure 5: Industry-wide Ransomware Victims

http://5aidibsmc4wt5l3lw4k5wtfqopbckllb3pntw7xw4qiem4a3eeacrlyd.onion/
http://atpimkcvvlvyizwazff6r5ioq6nnb7txijdwvlq4i6d5b7adx6c5egyd.onion/
http://xf7e5nnpiemhu6lpb5f723i4amgshhj33ny6c5ctbdjtc5duwtortoad.onion/
http://pol7t4rw4dymnyruiqkckbeul2xxntn7x3sek3yw553pxbwag3n4eeid.onion/
http://ondvd45cnciqs7fzu5ewm5li2ib75bppxjaapcyilceauq5xpmzbswad.onion/
http://mo3nqtrrrvguce64bvenu25uciry7buw2hzke4wxm22jhr57zmsj65qd.onion/
http://py5fgtglinssndrkrnbwgwjzxlsxl5zbyr3ypdiijgsllht2smznwpqd.onion/
http://jv2txdk66t6ijaugve3kte67yuahfaebrivy4okuqqvriaagsvi4pgad.onion/
http://enppltlenqakx4lyekcz5xmlhybemrii7l4gjnijs2mqvwr26jp73fad.onion/
http://gxru2ucw4yxkicwdiee6wpqwkogh2x3scfcnhcgb4lcyo4uid44734qd.onion/
http://pi25hxaofhsoxjh5g4e6iqcasoynlwygevqkbemzaalkyxwpgk77tqid.onion/
http://uzf4tt7buqhj5xzb7jnnmsd4wtufua4qyzjgjf4sn2vwniiqz5oi5lid.onion/
http://ftgvamayqmlyjkpf3dosoyfafbfpxxtxagsnt45sqauulckwupr2guid.onion/
http://lxgnxg3cdv4uq2ps4e5i66bykvol6rw7bsvr5chdpksusiqwhyx7cxqd.onion/
http://hqvcotd73c6hjfc3ogukvc37jgs2krmowyposqudq2rodtawmatxpyad.onion/
http://77k3qrvleqx3jn5mx73fpmhcfpk3pdrjs7tkgaxcsf4ojgizfhvmlhid.onion/
http://lejfkugm7arhigu2vhtcursl564e73gjrq23upuaccuafbj73rgbnfid.onion/
http://7kobff7iod6tmnyjgoqc4o367ufky2cvda4knnlvo2hakdzy4v4gffqd.onion/
http://obrze5nyt6pmx4ptffqliah7hxqb3je6jlghg7ynoy653nqvye43koid.onion/
http://tgcj6ad5dqmuayc7ldm3zw4bz3hx45nf54oe7vqtfs4hai4wsgbnseyd.onion/
http://4sw54rh5et4adx7oj6sl2kqkra243dq3dyhlxmoyt7vez6vncufv2gyd.onion/
http://oxbwvjzd2oc4cb4jkrnpwbuvabyj2pgmoh6q73jsuq35skfbta3p3uad.onion/
http://vksaeydmtcfee2qiwbdxb7lijqtwxzy55g4ft72vjvmjvxyuppskdwad.onion/
http://4s2org6ns4uhmamkr2tshq6f6auusktjjdoo23rskwhxfdlxlnx5rnyd.onion/
http://4dmex5fuyap32y6lkpglp5cy3ivoua452o57cezsxhfdlnhgvlw6sxid.onion/
http://m5ubrfq5bgwcckdxb3g3fcughlfntzv6kcvhw7bdkqsx7johtljefaqd.onion/
http://zlwljlbtakummd6biufuvljgqwbpvmrftd5kjtzxwjtn27jdzeahm5ad.onion/
http://tbgdp3msmgiddu7yhdo2fsuhlaggcoj3oez7wdmofznqm4dhevpekeyd.onion/
http://yiqfcld3loz7rh4kcmxrf4azyeqa7sonfyxqlnjjbxmmfxhzbm2vsjad.onion/
http://jhtym7doz6dt5xdq4dd5wuhmyaa6dtesv4lrnasb5scwofguffiewcqd.onion/
http://zdgj7z7dhmn5xgtrj4wh4gsf35hzst6blunfm3xf5iqpq6msiluxmmid.onion/
http://2yce6tllc6xin4kucqr4aynscfjsg7l7pgz3pv7rat5o3vjeruxpknid.onion/
http://xbpdja46coptbjt4a62lintyk547q54k7gubekbtsyqxivie4vln7syd.onion/
http://4hmvksa7vw5x3mytrguzcjxvj3alfbapxaekudmiigpztqxxv7dynnqd.onion/
http://2ynd4lgi277los7ykngk3my3rx3ehitx4agrpomrilwjic4iqisbikid.onion/
http://qiu5vqx2k3oyq3aeyz3pieh6g6yjzo7l5zofidxfvnahy3vgb2vuy6ad.onion/
http://gomf6ssy2bgsxlfbawncxdydwa4m76i4gzbwusmdwepuamx46uu6eqyd.onion/
http://fmrsmdsuokgzj5oujoqcod23gnvkqptg3vzbcqz6vw2ci7gonigijuyd.onion/
http://374ydckkglmslkqy3coatm5nn2rk3hg43lgci4wrhizhr47zfyfbdead.onion/
http://7izw24yz3udwtvfoq4lshv2ibow6jahx4lojoxsdt2nkqzzpr7osoxad.onion/
http://zz7ez3cgy6o4eehu5bc2cs7t4jvq7j7duragx3pfrgnafxui7l2ybzqd.onion/
http://kp5amzgfhwmpn26vnmx7h445x4xb7ofaxitonovt6mlewq5bpawkq7id.onion/
http://x3rx5uqoohqzfcnq3neiqwunb6eh5yc4ybu26nxwqqltclkvdvwbprad.onion/
http://2f7k6jhxwbpiyuomb27eywzollahlje2xph3t5wckupkoeluantatbad.onion/
http://tlr5h3my4jyvwgmyrvu2oadls2o3f377cz2bqnu3g7oaycofiweqjfyd.onion/
http://ib3ru7m66tg37w6o7zxe4upntw2p7236c63wb5n3beeapiuor535vhad.onion/
http://rivdgsucnasob3iiux5j4g4ybqz6flxgx2vz4h6i2wfu42hbbmwwcuqd.onion/
http://dfhu2iceszxurn7lf5mb5xhainmb7vulpizncjomtn4w5j5cv3pz52qd.onion/
http://2ntyvlixm5zzhn2zgowgbbu5s6forpttomntefg5dapivr5qwokkyvyd.onion/
http://uax2s63op7lboqhuxscjfiwcea4retnus6z2ph33cd44dyqdsyosj6id.onion/
http://w6kf2ktnbzx3hha25snxdwg57ydqdskzcs5tdrdztajb2vn7jk5hzrid.onion/
http://vokr3ancppaevval5hwpqpm43szyj7nysfoxqfsrc274jabs5m2227yd.onion/
http://mdpkohdcvgyiexi4yihiufdi2wmau5yd6wjr7rituvwntifxuh43deyd.onion/
http://iwtkvmhwx7g743ytqj6yiibbb33a3ycezssyn6gai2hny7b2ynez6sad.onion/
http://uiecrea6byqjfppofxjcku2rjs6qxeqblnc7ljveopbtd4ih635saiid.onion/

http://n7f7ic7islqbyw3vzans3mddgaooirbf4i75tvsfvxjvni7vxanwczad.onion/
http://utijlj5t2xamyekjr3ur7vpdnttaqit57fher2nzibih3nqil75jhjyd.onion/
http://lc6wrbsdvaayqkhj47bjkj7mfnaiyvsnufmdnkhai6de3uxhu6bssgyd.onion/
http://nxml7szv4m3hd6gtjjg62xejyusbbqvmb3thfwaa6wimablrzuk7p3qd.onion/
http://jt772jtwpfrluifvz34ti43kfgv6lz7bgiviwopl73slo6a3wetch4yd.onion/
http://2xipgq7vsu6d6llgg4tr4wxwdc5tbmmtx3jxfax3kx2dorkcnzsimwqd.onion/
http://d7akeguwmrxmrg7tgzx7a73mksq3zpcjjk2c4jibfhmvrhhd6oprsfyd.onion/
http://ozokx66qqmtvjbkbkudtfnrfy5euwug2gbekqm6ug42j76knmtzcrkid.onion/
http://yj2xh4wxcjncsgj7642jzky7uf4mrjcp6zrcdgxylxbepyvgv4meljqd.onion/
http://l2abuimje7jrypvv57p2ihf36rza2etoobyvsddgxqrsssn7tyb7txid.onion/
http://43xvcojnfpqlbjxrbuuulyh3xtqrkl3qboi67xxd4jsigmpccbhxcoid.onion/
http://6ibv6c5n6orfgzpt4apgqtrbr3ot2ninpbpi6hwolq2lzcgj6lzj4rid.onion/
http://kinkwgtp4sfj3tovixjlvsklktjul7v5o55lkf6cgmlnugqlletzsxad.onion/
http://k2xhcuvhwh5cyua5vwa4xjeyvyfatzkrh5yn5kc5munvglzge4cod2ad.onion/
http://zv7u2tclxajbgae6ba4jkisnkfkts3lk7lxlypmuqktrk42qmo2c7hqd.onion/

Chat servers

http://secxrosqawaefsio3biv2dmi2c5yunf3t7ilwf54czq3v4bi7w6mbfad.onion/