cyberthint

RANSOMWARE REPORT

JULY

2024 JULY

PREPARED BY CYBERTHINT THREAT HUNTERS

CYBERTHINT.IO

Table of Contents

Introduction

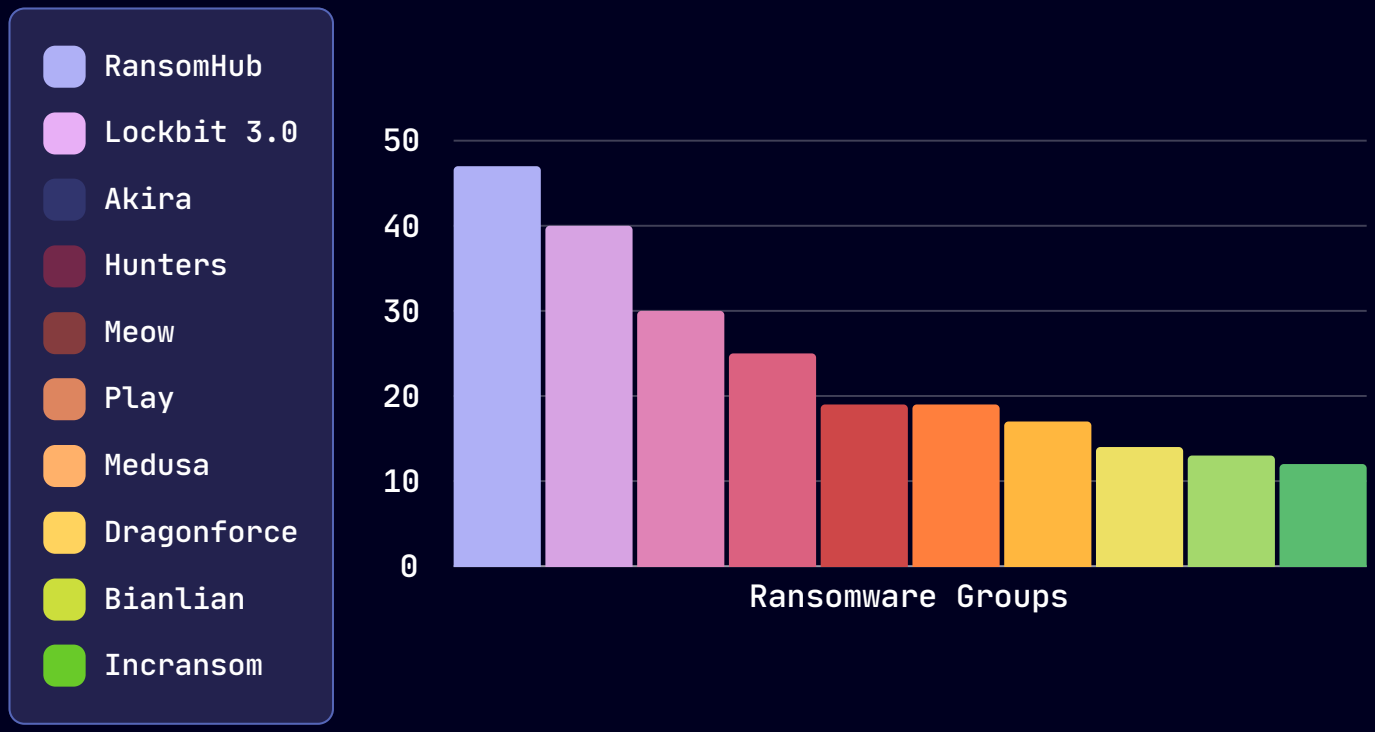
Welcome to Cyberthint's monthly Ransomware Tracking report, a compilation of statistical data gathered as Cyberthint threat hunters closely monitor the activity and behavior of ransomware groups.

Cyberthint threat hunters use the following six-point methodology when tracking ransomware groups on the Darkweb.

#	Ransomware Tracking Methodology
1.	**Collecting Data Sources:** We collect all data from sources related to ransomware groups operating on the Darkweb.
2.	**Data Analysis and Classification:** We analyze the data collected from the related sources and classify them according to ransomware groups.
3.	**Examination of Distribution Methods:** We analyze the distribution methods and strategies of ransomware groups using the available data that we have.
4.	**Monitoring Ransomware Campaigns:** By tracking large-scale ransomware campaigns, we observe changes in strategies adopted by ransomware groups.
5.	**Monitoring Ransom Payments:** We track crypto wallets that we have identified as belonging to ransomware groups and in this way, we can predict the sectors and countries they may target in the future.
6.	**Protection and Recommendations:** Based on the data and statistics collected and analyzed during Ransomware Tracking, we identify measures to safeguard against these attacks.

Most Active Ransomware Groups

Cyberthint threat hunters have identified the top 10 ransomware groups that made the most attacks in July as a result of the data they collected. This data is sourced from victim announcements shared on the groups' Darkweb websites, and attacks not announced on these sites are not included in this analysis.

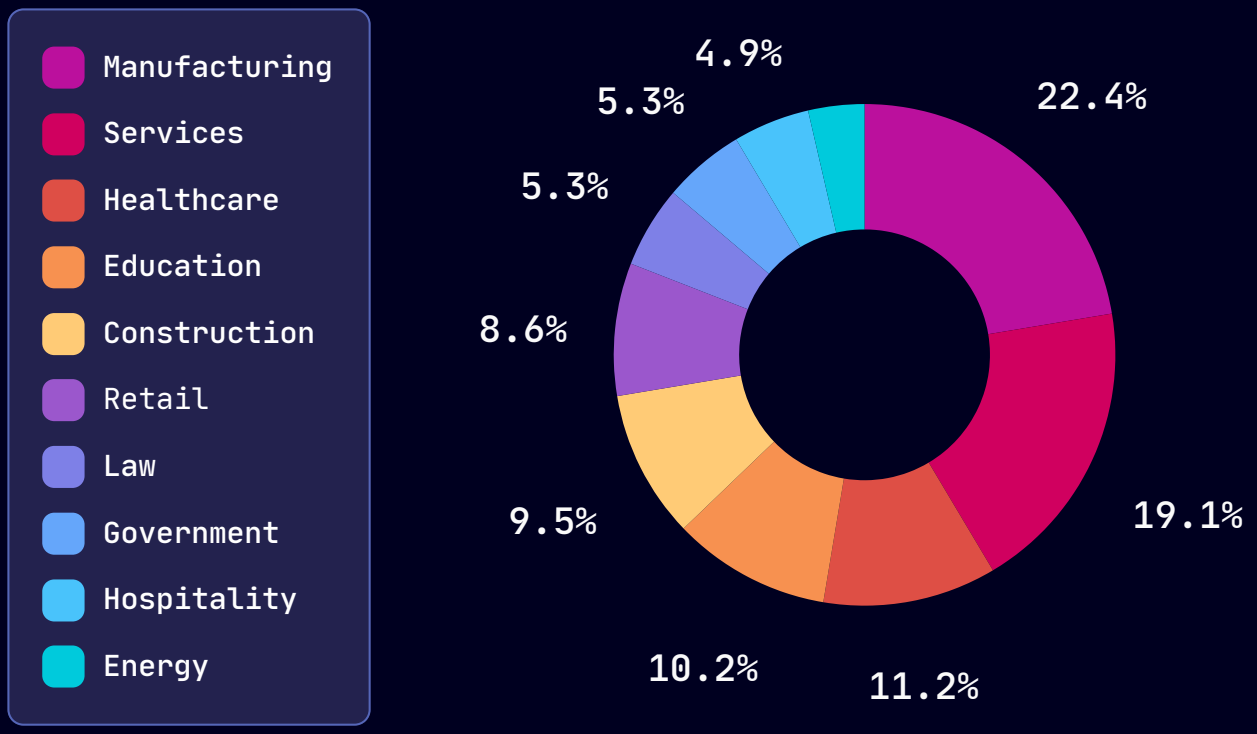


Ransomware Attacks Increased in July

Ransomware attacks increased by 20% compared to June. A total of 409 ransomware attacks were recorded in July.

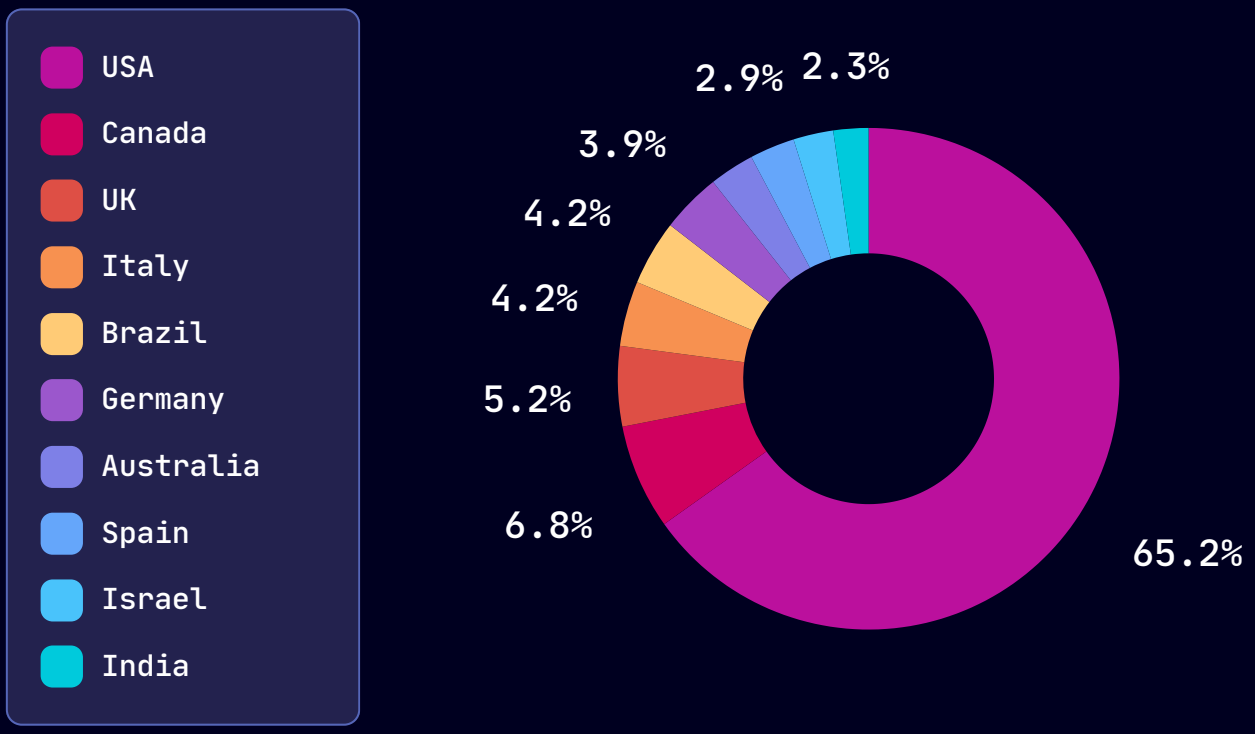
Sectors Most Affected by Ransomware Attacks

Cyberthint threat hunters have identified based on the collected data the sectors most targeted by ransomware attacks in July. This data is derived from victim announcements posted by ransomware groups on their own websites on the darkweb, and does not include attacks that they did not announce on their websites.



Countries Most Affected by Ransomware Attacks

Cyberthint threat hunters collected data to identify the countries that suffered the most ransomware attacks in July. This data is derived from victim announcements posted by ransomware groups on their own websites on the darkweb, and does not include attacks they did not announce on their websites.



A Variant of PLAY Ransomware Affecting VMWARE ESXI Servers Detected

The Lockbit ransomware gang made a post announcing that they have violated the Federal Reserve (aka The Fed) on 23 June via their leak website. "33 terabytes of juicy banking information containing Americans' banking secrets," the Lockbit gang said, claiming to have stolen 33 Terabytes of data. After a while, the group started to publish the allegedly stolen data on its website. As a result of the research, it was revealed that the data shared was not Fed data, but data leaked from another financial institution. A spokesperson for Evolve Bank & Trust, the institution from which the data was leaked, stated that they will offer free credit monitoring with identity theft protection services to all customers affected by this incident and that they are deeply investigating the leak.

Ransomware Actor Who Hacked NASA Has Reward For His Detention

A Kansas hospital lost access to its server hosting X-rays and other diagnostic images and was forced to cancel patient appointments as a result of a ransomware attack in 2021. Threat actors targeted at least five American healthcare organisations using malware developed by North Korea's military intelligence agency.

In the indictment returned by a grand jury in Kansas City, Rim Jong Hyok is accused of targeting NASA, US military bases and healthcare facilities, as well as defence and energy companies in China, Taiwan and South Korea. It is stated that Rim and his accomplices worked for the General Bureau of Reconnaissance, North Korea's military intelligence agency, known in the private sector as "Andariel", "Onyx Sleet", "APT45".

"Rim Jong Hyok and his co-conspirators deployed ransomware to extort U.S. hospitals and health care companies, then laundered the proceeds to help fund North Korea's illicit activities," said Deputy Director Paul Abbate of the FBI. "These unacceptable and unlawful actions placed innocent lives at risk. The FBI and our partners will leverage every tool available to neutralise criminal actors and protect American citizens."

Rim and its alleged member Andariel reportedly gained access to NASA's computer system for more than three months, obtaining more than 17 gigabytes of unclassified data. They also gained access to the systems of defence companies in Michigan and California, as well as Randolph Air Force base in Texas and Robins Air Force base in Georgia, officials said.

The US State Department has offered a $10 million reward for information leading to the discovery of North Korean Ransomware actor Rim Jong Hyok or other foreign government officials targeting US critical infrastructure.

Blood Donation Centre in the US Suffered OneBlood Ransomware Attack

On Monday 29 July, OneBlood, a non-profit blood donation organisation serving hundreds of hospitals in the southeastern United States, was hit by a ransomware attack. The attack affected OneBlood's software system.

After the attack, the organisation stated that it carried out its normal operations and procedures manually as much as possible. In its statements, the organisation called on users to donate blood as it worked with significantly reduced capacity after the ransomware attack. In the rest of their statements:

"OneBlood takes the security of our network extremely seriously. Our team reacted quickly to assess our systems and began an investigation to confirm the full nature and scope of the event," said Susan Forbes, the senior vice president of corporate communications and public relations at OneBlood, in a statement. "Our comprehensive response efforts are ongoing and we are working diligently to restore full functionality to our systems as expeditiously as possible."

Los Angeles County Court Forced to Shut Down Network Systems Due to Ransomware Attack

The Los Angeles County Superior Court, which serves nearly 10 million people and is the largest unified court in the United States, has been hit by a ransomware attack.

The Los Angeles County Superior Court said the attack was first detected on the morning of Friday 19 July. Upon detection of the attack, court officials disabled their network systems.

"The Court experienced an unprecedented cyber-attack on Friday which has resulted in the need to shut down nearly all network systems in order to contain the damage, protect the integrity and confidentiality of information and ensure future network stability and security," said Presiding Judge Samantha P. Jessner.

SUPERIOR COURT OF CALIFORNIA
COUNTY OF LOS ANGELES

NEWS RELEASE

COMMUNICATIONS OFFICE

www.lacourt.org | publicinfo@lacourt.org | @LASuperiorCourt

Media Relations
publicinfo@lacourt.org

FOR IMMEDIATE RELEASE:
July 19, 2024

SUPERIOR COURT OF LOS ANGELES COUNTY EXPERIENCES RANSOMWARE ATTACK

On Friday, July 19, 2024, the Superior Court of Los Angeles County's Court Technology Services (CTS) Division identified a serious security event in the Court's internal systems which has now been determined to be a ransomware attack. The attack began in the early morning hours of Friday, July 19. The attack is believed to be unrelated to the CrowdStrike issue currently creating disruptions to technology platforms worldwide.

Immediately upon discovery of the attack, the Court disabled its network systems to mitigate further harm. The Court's network systems will remain disabled at least through the weekend to enable the Court to further remediate the issue. The Court is receiving support from the California Governor's Office of Emergency Services (CALOES) as well as local, state and federal law enforcement agencies to investigate the breach and mitigate its impacts. At this time, the preliminary investigation shows no evidence of court user's data being compromised.

Over the past few years, the Court has invested heavily in its cybersecurity operations, modernizing its cybersecurity infrastructure and making strategic staff investments in the Cybersecurity Division within CTS. As a result of this investment, the Court was able to quickly detect an intrusion and address it immediately.

Due to the ongoing nature of the investigation, remediation and recovery, the Court will not comment further until additional information is available for public release.

Further information on impacted court operations and services will be shared as it becomes available.

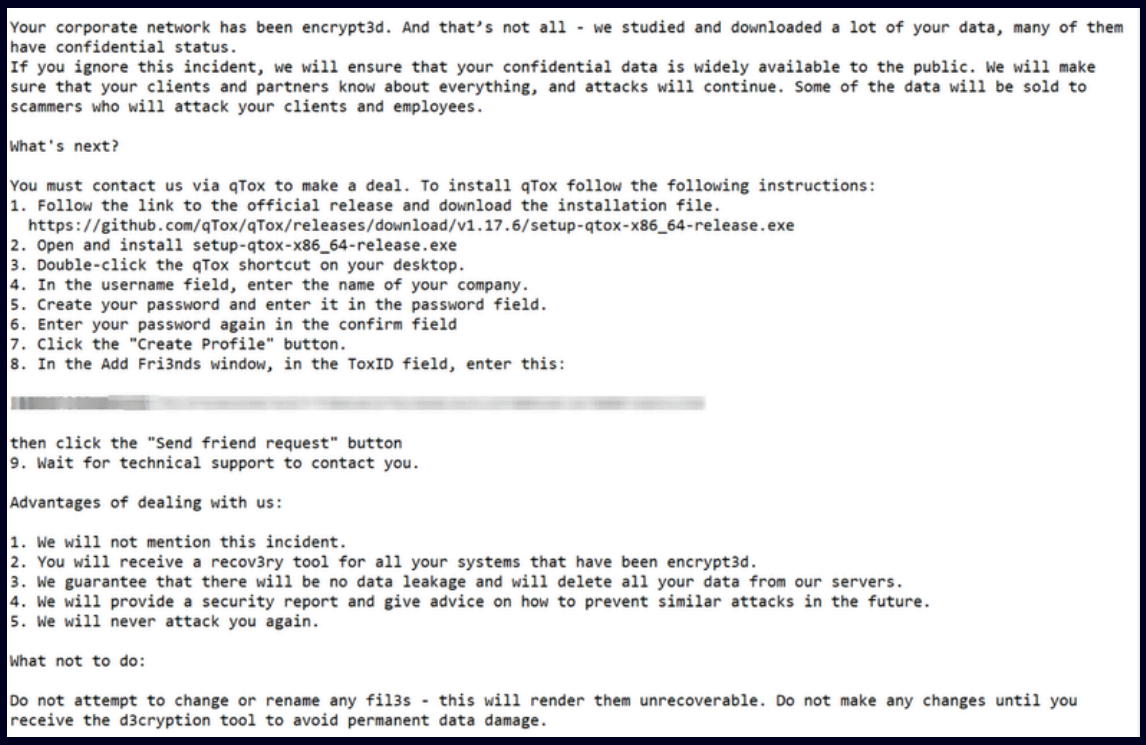
Please follow the Court on 'X', @LASuperiorCourt, and Instagram, @LASuperiorCourt, for the latest updates.

Court officials declined to answer questions about how the attackers gained control of the systems, whether they paid a ransom, what confidential information, if any, was exposed, or whether any data was lost. Court online operations remained closed until 23 July. In the following dates, the systems that were active again with updates were gradually activated.

New Ransomware Group: "Volcano Demon"

The newly revealed Volcano Demon ransomware group uses phone calls for ransom demands. Unlike other ransomware groups, threat actors do not have a leak site. Researchers say that so far the group has carried out two known successful attacks.

Before calling, threat actors encrypt files on victims' systems with LukaLocker ransomware with the .nba file extension and leave a ransom note. The note states that they encrypted the victim's corporate network and examined and downloaded their data. They threaten to leak the data if they ignore them.



```
Your corporate network has been encrypt3d. And that's not all - we studied and downloaded a lot of your data, many of them
have confidential status.
If you ignore this incident, we will ensure that your confidential data is widely available to the public. We will make
sure that your clients and partners know about everything, and attacks will continue. Some of the data will be sold to
scammers who will attack your clients and employees.

What's next?

You must contact us via qTox to make a deal. To install qTox follow the following instructions:
1. Follow the link to the official release and download the installation file.
  https://github.com/qTox/qTox/releases/download/v1.17.6/setup-qtox-x86_64-release.exe
2. Open and install setup-qtox-x86_64-release.exe
3. Double-click the qTox shortcut on your desktop.
4. In the username field, enter the name of your company.
5. Create your password and enter it in the password field.
6. Enter your password again in the confirm field
7. Click the "Create Profile" button.
8. In the Add Fri3nds window, in the ToxID field, enter this:

[redacted]

then click the "Send friend request" button
9. Wait for technical support to contact you.

Advantages of dealing with us:

1. We will not mention this incident.
2. You will receive a recov3ry tool for all your systems that have been encrypt3d.
3. We guarantee that there will be no data leakage and will delete all your data from our servers.
4. We will provide a security report and give advice on how to prevent similar attacks in the future.
5. We will never attack you again.

What not to do:

Do not attempt to change or rename any fil3s - this will render them unrecoverable. Do not make any changes until you
receive the d3cryption tool to avoid permanent data damage.
```

It is not yet clear if the group is part of a known Ransomware organisation.

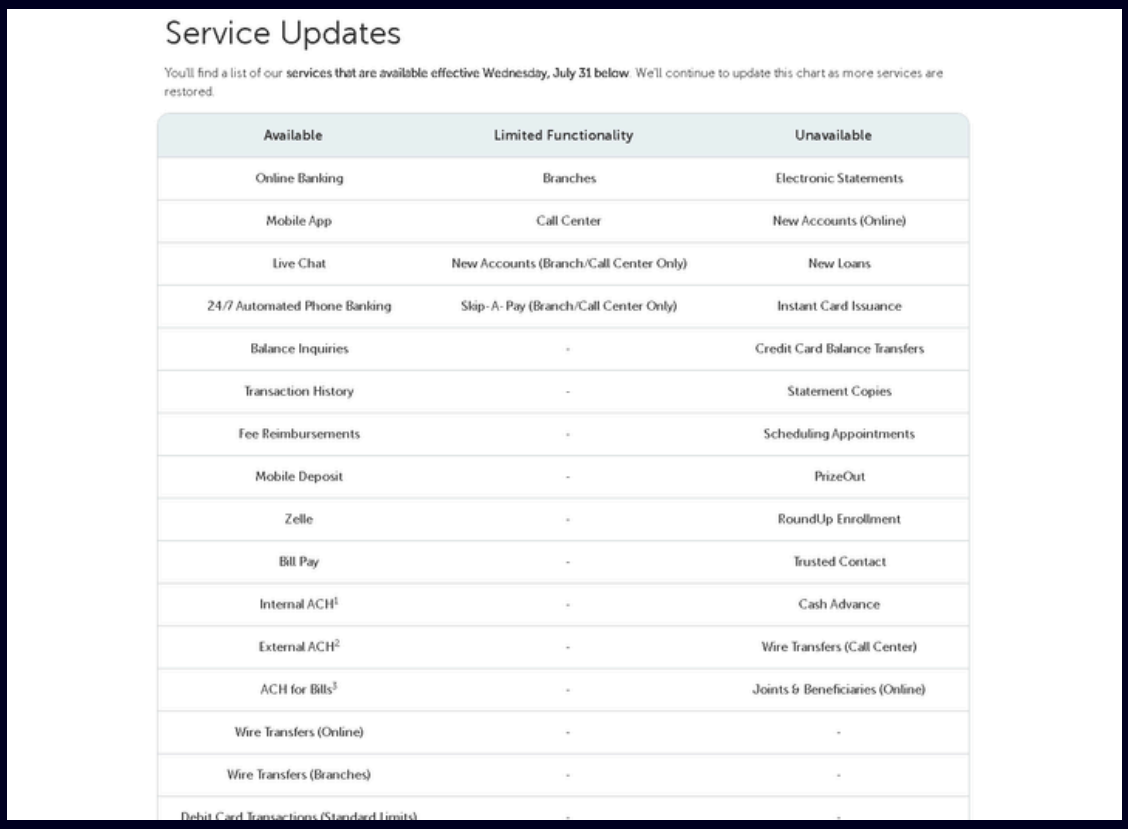
Impacts of Cyber Attack on Patelco Still Ongoing

On 29 June, Patelco Credit Union, which serves half a million members through 37 branches with approximately $10 billion in assets, was hit by a ransomware attack. On the fifth day of the breach, the company's CEO confirmed that they had experienced a ransomware attack.

The attack caused Patelco to suspend electronic transfers, balance inquiries and direct deposits. The credit union was also forced to limit debit and credit card transactions for its members.

While the company's CEO said members' funds were "safe and secure" and other services would be restored shortly, he did not disclose whether any personal data had been breached.

The company publishes the latest updates on the process on their website. According to the latest update published on 31 July, there are still services that are unavailable and have limited access.



Service Updates

You'll find a list of our **services that are available effective Wednesday, July 31 below**. We'll continue to update this chart as more services are restored.

Available	Limited Functionality	Unavailable
Online Banking	Branches	Electronic Statements
Mobile App	Call Center	New Accounts (Online)
Live Chat	New Accounts (Branch/Call Center Only)	New Loans
24/7 Automated Phone Banking	Skip-A-Pay (Branch/Call Center Only)	Instant Card Issuance
Balance Inquiries	-	Credit Card Balance Transfers
Transaction History	-	Statement Copies
Fee Reimbursements	-	Scheduling Appointments
Mobile Deposit	-	PrizeOut
Zelle	-	RoundUp Enrollment
Bill Pay	-	Trusted Contact
Internal ACH[1]	-	Cash Advance
External ACH[2]	-	Wire Transfers (Call Center)
ACH for Bills[3]	-	Joints & Beneficiaries (Online)
Wire Transfers (Online)	-	-
Wire Transfers (Branches)	-	-
Debit Card Transactions (Standard Limits)	-	-

Octo Tempest Ransomware Expands Their Arsenal

Microsoft announced that Octo Tempest has added two more ransomware payloads, Qilin and RansomHub, to its arsenal.

Founded in early 2022, Octo Tempest initially focused on SIM swaps and stealing cryptocurrency-rich accounts. It later became a subsidiary of ALPHV/BlackCat in mid-2023.

By June 2023, the group began distributing ALPHV/BlackCat ransomware payloads to victims, targeting VMWare ESXi servers. It speculates that the addition of new payloads may be due to BlackCat no longer being in use.

Ways to Prevent Ransomware Attacks

1. **Use Strong Passwords:** Create complex, long and unique passwords for each account.
2. **Don't Ignore Software Updates:** Regularly update the operating system, applications, services and antivirus programs.
3. **Use Antivirus and Security Software:** Regularly scan your system for malware using reliable antivirus software.
4. **Beware of Emails:** Avoid clicking on suspicious email attachments or links.
5. **Secure File Sharing:** Share your files using trusted and secure sharing platforms.
6. **Backup Data:** Back up all your important data regularly. Also pay attention to the security of the backup.
7. **Training and Awareness:** Educate yourself and your employees about ransomware and cyber threats.
8. **Use Advanced Authentication:** Increase the protection level of your accounts by taking additional security measures such as two-factor authentication.
9. **Network Security:** Protect your network using firewalls, network monitoring and security solutions.
10. **Malware Protection:** Take effective measures to detect and block malware that may be come via email, web and other means.
11. **Application Permissions:** Do not give unnecessary permissions to applications and files. You can defend against attacks by restricting permissions you don't need.
12. **Download from Trusted Sources:** Download software and applications only from official and trusted sources. Stay away from pirated or suspicious sources.

Checklist During a Ransomware Attack

1. Isolate Infected Systems: Immediately isolate affected systems from the network to prevent the ransomware from spreading further.

2. Alert Management: Notify relevant stakeholders, including management, legal, and IT teams, about the attack.

3. Gather Information: Document all available information about the attack, including the ransom note, malware samples, and affected systems.

4. Engage Incident Response Team: If available, involve your incident response team to lead the investigation and recovery efforts.

5. Assessment: Determine the scope and impact of the attack on your systems and data.

6. Containment: Identify the ransomware variant and apply appropriate measures to contain the attack, such as disabling compromised accounts or network segments.

7. Data Backup Check: Verify the integrity of your data backups to ensure they are not compromised. Use clean backup data for recovery.

8. Communication Plan: Develop a communication plan for informing employees, customers, and partners about the situation, while adhering to legal and regulatory requirements.

9. Malware Analysis: Conduct analysis on the ransomware to understand its behavior, possible decryption methods, and potential vulnerabilities.

10. Engage Law Enforcement: If necessary, involve law enforcement agencies and share relevant information with them.

11. Recovery Strategy: Develop a recovery strategy based on the nature of the attack, whether it's possible to decrypt files, or if you need to rebuild systems from scratch.

12. Negotiation Consideration: Evaluate the risks and benefits of negotiating with the attackers for decryption keys. This is a complex decision with legal and ethical considerations.

13. User Education: Reinforce user education on cybersecurity practices to prevent future attacks.

14. Patch and Update: Identify and patch vulnerabilities that were exploited to deliver the ransomware.

15. Monitor and Analyze: Continuously monitor for signs of the ransomware reactivating or any new vulnerabilities being exploited.

16. Forensics: Conduct a thorough forensic analysis to understand how the attack occurred and whether any data was exfiltrated.

17. Post-Incident Review: After the attack is contained, conduct a review of the incident response process to identify areas for improvement.

18. Risk Mitigation: Implement security measures to prevent similar attacks in the future, such as endpoint detection and response (EDR) solutions, email filtering, and user training.

How Cyberthint Can Help You To Prevent Ransomware Attacks

Data Leakage Monitoring

It regularly inspects whether there is a data leak related to your organization. If it detects anything, it notifies you.

Attack Surface Detection

Every asset open to the internet is a potential attack point. Cyberthint detects them for you and notifies you of potential breach points.

Vulnerability Intelligence

It notifies you about the vulnerabilities detected by regular vulnerability scans with its solutions.

Brand Monitoring

It detects potential phishing attacks on you and your employees by impersonating your organization in advance and takedown the impersonated/fake; domain name/social media account before the attack can be made.

We know what information hackers have on you!

Cyberthint is an unified cyber threat intelligence platform that allows you to take precautions against cyber threats that may affect your company and employees in cyberspace.

Be aware of cyber threats targeting your organization in advance with Cyberthint's advanced cyber threat intelligence technology!

With Cyberthint, you can monitor and identify advanced threats and take early action.

Follow Us Cyberthint.io Cyberthint Cyberthint Cyberthint