certnz

Q2

APRIL_TO_JUNE_2022

CYBER SECURITY INSIGHTS

Banking on a disguise

IN THIS ISSUE

Te Kāwanatanga o Aotearoa
New Zealand Government

Q2 CYBER SECURITY INSIGHTS

Director's message

Rob Pope, Director

On the surface it might look like nothing much has changed, with incident numbers remaining steady and only a small increase in direct financial loss – but it's been another busy quarter across the threat landscape, and every incident reported has had an impact on people and businesses.

The recent spate of phone-spoofing scams targeting bank customers saw us working alongside financial institutions, telecommunication providers and other government agencies. Collaborating meant we could better understand the technology behind the scams and how to help stop them, as well as developing clear and consistent advice for banking customers.

In this quarter's report, we highlight the importance of collaboration and knowledge sharing in helping New Zealanders better protect themselves online.

The more information and insights we have, the stronger our advice and mitigations are. This goes beyond large organisations too—everyone can play a part. By reporting cyber security incidents to CERT NZ, New Zealanders are helping others from being impacted by giving us the indicators and understanding of how these attackers are working. This means we can work collectively with our partner organisations to reduce these harms and raise awareness of cyber security threats.

That can be simple guidance on how to identify a scam call through to technical controls for securing internet exposed devices. And while the latter example is based on technology vulnerabilities, in many ways, cyber security is centred on people.

As covered in this report, attackers may use technology to initiate an attack, but they also rely on New Zealanders' trusting nature to carry out their scam. Being a cyber resilient Aotearoa isn't just about technology, it's about making sure everyone has the basic tools at their disposal to be secure online.

AT A GLANCE...

Average incidents reported per quarter

2,234

Average loss reported per quarter

$4.2m

Losses reported to CERT NZ from previous eight quarters

$33.6m

Figures based on previous eight quarters

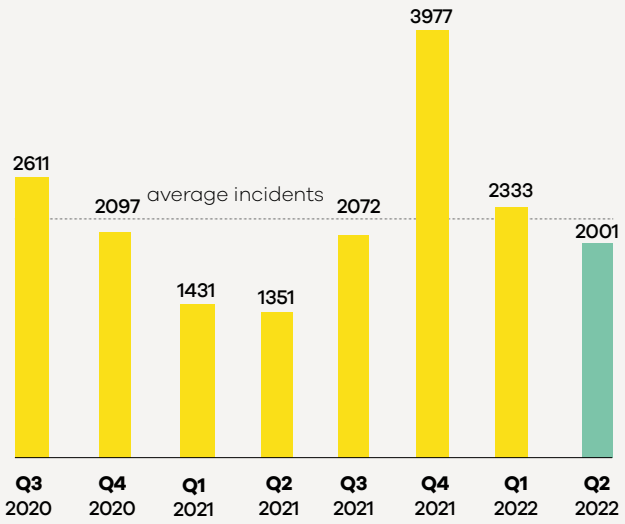
INCIDENTS RESPONDED TO BY CERT NZ

2,001

incidents were responded to by CERT NZ in Q2 2022.

▼14%

decrease from Q1 2022.



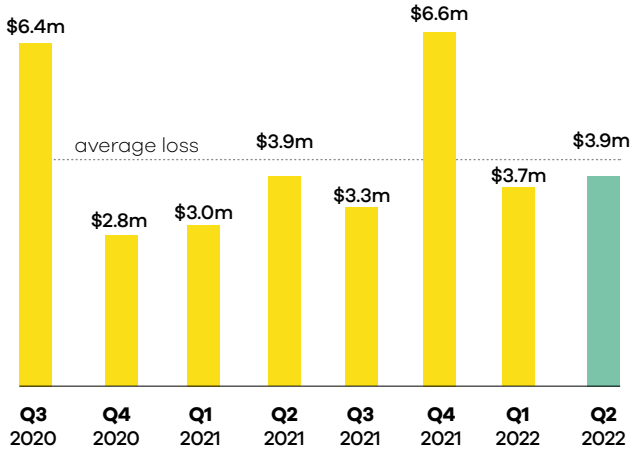
DIRECT FINANCIAL LOSS

$3.9m

in direct financial loss was reported in Q2 2022.

▲5%

increase from Q1 2022, with 19% of incidents reporting financial loss.



BREAKDOWN BY INCIDENT CATEGORY

In Q2 there was a decrease in report numbers across most incident categories. Despite the decrease, there was a 5% increase in direct financial loss.

		From previous quarter
Phishing and credential harvesting	1116	▼ 19%
Scams and fraud	526	▼ 6.9%
Unauthorised access	230	▲ 0.9%
Malware	62	▼ 23%
Website compromise	13	▼ 46%
Ransomware	5	▼ 71%
Botnet traffic	2	▼ 71%
Denial of service	2	▼ 50%
C and C server hosting	1	▼ 75%
Suspicious traffic	0	▼ 100%
Attack on system	0	● 0%
Other	44	▲ 38%

For more on the New Zealand threat landscape in Q2 2022, see the CERT NZ Quarter Two: Data Landscape.

Banking on a disguise

In quarter two, CERT NZ became aware of a spike in scam calls where attackers were pretending to be from a bank to try and trick recipients into sharing financial information, giving access to their bank accounts or allowing remote access to their devices or PCs.

Attackers are constantly evolving techniques to try and catch people out. In these specific scam calls, they use ‘phone spoofing’ software which changes out the scammer’s actual phone number and instead shows a phone number of the scammer’s choosing (like a bank’s phone number) on the recipient’s caller ID.

CERT NZ is aware of New Zealanders losing large sums of money to these types of scams, with some recipients experiencing these incidents more than once – this happens when scammers call back, pretending to be from the bank and offering help to recover from the previous scam.

New Zealand banks have worked with telecommunication providers and the New Zealand Telecommunications Forum (TCF) to block their numbers from being spoofed.

CERT NZ and New Zealand banks are now aware that scammers have further evolved the approach by changing out one or two numbers to closely imitate the banks’ phone numbers.

HOW IT IS HAPPENING

1. The scammers use intermediary software that generates signals to change the displayed caller ID.

2. Once the attacker has the target on the phone, they use social engineering tactics to try and get the financial information or access they are seeking.

3. To sound more plausible, attackers are often using scripts and dialogue similar to those used by the bank call centres. In many cases, they pretend to be from a bank's fraud centre and say they've detected unauthorised access of the recipient's account. In some cases, they use fear or urgency to get the recipient to act quickly.

HOW TO TELL IF YOU'RE BEING CALLED BY A SCAMMER

If you receive a phone call from a person claiming to be from your bank, even if the phone number looks similar to the bank's phone number, there are some red flags that can help you identify if the call is legitimate.

With a bank scam call, the scammer will usually do one of the following.

Ask the recipient to download remote-access software under the pretext of being able to walk the customer through a necessary process.

Trigger a SMS code that is sent to the recipient's phone. This is a code to either gain access or authorise a transfer, but the attacker will say it is a 'cancellation code' or something similar, and ask the recipient to read it out.

Ask for the recipient's bank account log in information or full credit card number.

"Attackers are often using scripts and dialogue similar to those used by bank call centres."

WHAT TO DO IF YOU THINK IT'S A SCAM CALL

CERT NZ strongly recommends ending the call and hanging up if you have any concerns about the legitimacy of a call.

Then find the bank's phone number from the bank's website or on the back of your bank card, and call them. This way you'll find out if the original call was genuine.

In some cases, when a recipient tries to end a call, the scammer will use fear and urgency tactics to try and convince the recipient to stay on the call and respond to the request.

Protect yourself and your bank accounts from scam calls

Enable two-factor authentication (2FA) on your bank account[1]. This adds an extra security layer on top of your password, like a code sent to your phone. That way if an attacker gets your login details, they still won't be able to access your account.

Never share these codes with anyone. Your bank will never ask you for a 2FA code.

If you have clicked on a suspicious link or received a call where you've provided a 2FA code, contact your bank immediately and report the incident to CERT NZ. **www.CERT.govt.nz**

Never give out account information, credit card details or remote access to your devices. Your bank will never ask for this information.

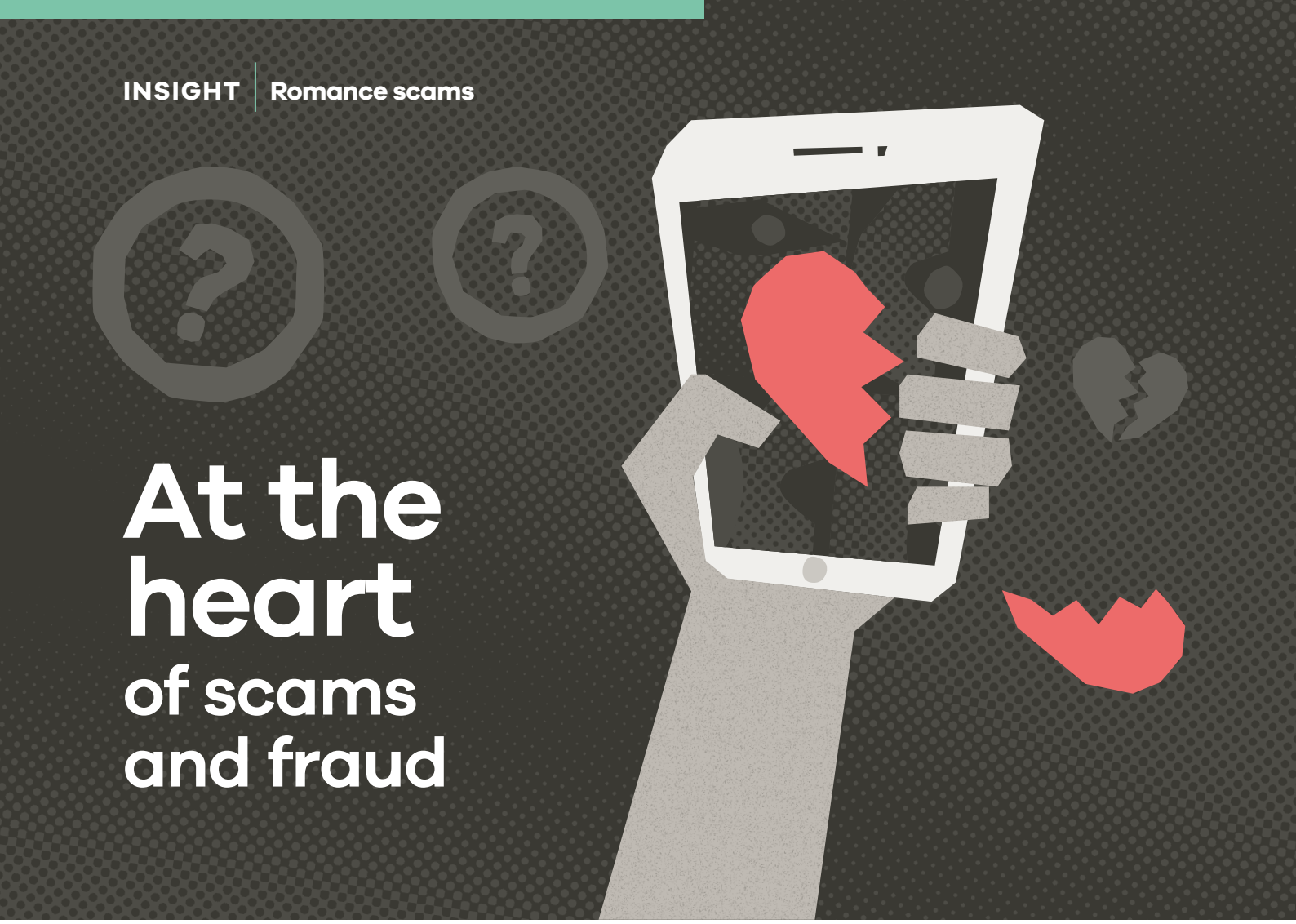
HOW CERT NZ IS HELPING COMBAT PHONE SPOOFING

CERT NZ works with other New Zealand organisations, like financial institutions, to combat scam calls. We share information and insights to better understand who is being targeted and the tactics scammers are using. This information helps put a stop to these calls taking place, and also helps us develop relevant advice and mitigations so New Zealanders can better protect themselves from being impacted.

In June, CERT NZ, New Zealand banks and the Department of Internal Affairs (DIA) released a media statement to educate the public on these scam calls[2].

Where possible, CERT NZ passes the details of scam calls to the Telecommunication Forum (TCF), so they can investigate the calls and the scammers can no longer use those phone numbers.

[1]https://www.cert.govt.nz/individuals/guides/two-factor-authentication/
[2]https://www.cert.govt.nz/individuals/news-and-events/scammers-using-sophisticated-attacks-against-new-zealanders/



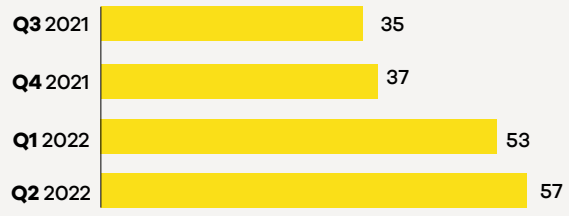
At the heart of scams and fraud

Scams and fraud is consistently one of the most reported categories to CERT NZ.

In quarter two, New Zealanders reported over 500 incidents about scams and fraud, and 92% of these reports (486) were about individuals – with a total direct financial loss of $3.2 million.

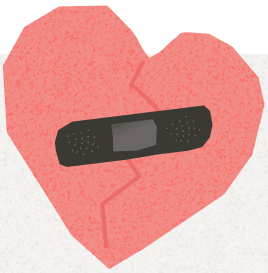
Of the types of scams and fraud reported, 'buying and selling of goods online' is consistently the most reported. This quarter, 'dating and romance scams' was the second most reported, with the number of incidents in this category steadily increasing across the past four quarters.

ROMANCE AND DATING SCAMS REPORTS



ROMANCE SCAMS

A romance scam is when a scammer takes advantage of someone looking for a relationship online. Scammers will use dating websites and apps or social media to build a relationship with someone. Once they've gained the person's trust, the scammer will start to ask for money, gifts, personal details or they will make unusual requests that can be used to commit fraud or to exploit the individual. More recently, CERT NZ has seen reports where romance scammers are building trust to try and trick the individual to buy into crypto investment scams. The scammers often use fake profiles to make it harder to track them down.



PREVENTIONS, CHECKS AND RED FLAGS

Avoid giving out too much personal information online, including on social media or by email.

If you're unsure about a connection, reverse image search can help identify if the image has been used elsewhere or doesn't match the identity of the person they are claiming to be. You can do this by uploading the image to a search engine.

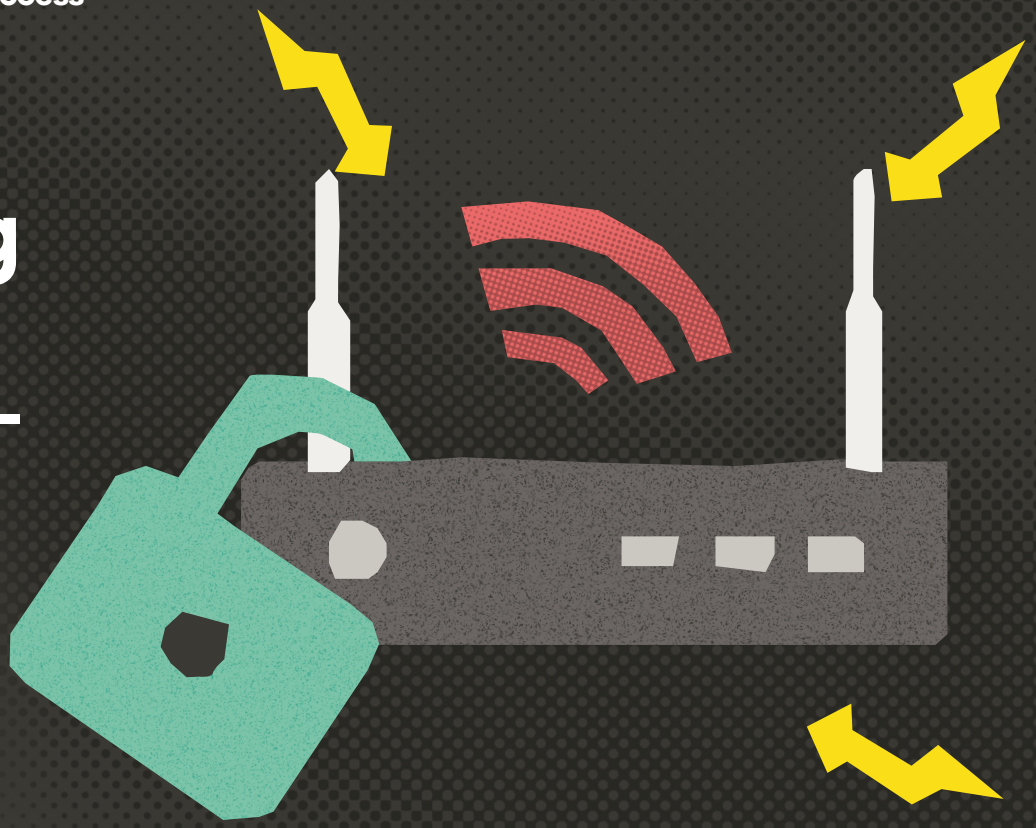
Avoid responding to requests for financial help, making investments or sending money. This includes sending money to enable them to meet you in person.

Sometimes there are multiple scammers working together, look out for inconsistency in communication style.

If the contact is not willing to meet up or talk via video call, or comes up with a series of excuses to avoid meeting, they could be a scammer.

If you think you may have experienced a romance scam or are concerned about a connection you've made, we can help. Please report confidentially to CERT NZ. www.CERT.govt.nz/report

Reducing the risk of internet-exposed services



This quarter, CERT NZ received 230 reports about unauthorised access. This is when an attacker gains access to an account, a service or a device usually through vulnerabilities in software, or weak or stolen credentials.

Over the past four quarters, New Zealanders have reported $3 million in direct financial losses to this incident type. It can also cause significant impacts including operational, reputational and data loss.

One avenue for attackers to gain unauthorised access is through - internet-exposed services, like Remote Desktop Protocol (RDP), Network Attached Storage (NAS) devices, websites and databases. Once the attacker has gained access, they can carry out a number of malicious actions. The most significant actions can include running commands on a device remotely, deploying ransomware[3] and stealing data and money. These can be costly and time consuming to recover from.

WHY SERVICES MAY BE AT RISK

Exposing a device or service on the internet is not just connecting it to the internet but allowing someone to connect directly to your device from the internet. This can happen intentionally through port forwarding, port triggering, or a 'demilitarised zone' (DMZ) or unintentionally due to a poorly configured network firewall or missing network firewall. Attackers can only exploit what they can access. If you expose a service or device on the internet, it can be much easier to access.

"Exposing a device or service on the internet is not just connecting it to the internet but allowing someone to connect directly to your device from the internet."

[3]See 'Ransomware attacks targeting network attached storage devices' https://www.cert.govt.nz/about/quarterly-report/quarter-one-cyber-security-insights-2022/

HOW TO REDUCE RISK IN YOUR BUSINESS

Many New Zealand businesses, small and large, use - internet-exposed services.

The following mitigations may require some technical ability. If you are unsure whether they relate to your business, CERT NZ recommends checking with your IT provider

- **Identify what is exposed to the internet** to help mitigate this risk, it's important to identify what is being exposed to the internet. Asset Lifecycle Management[4] can help you do this. You can also use scanning tools like Nmap and Nessus to help assess your situation.

- **Only expose what you really need to** Reducing the number of services you use[5] lowers the number of targets that attackers have access to. This is known as reducing your attack surface.

  If you do need to expose services, CERT NZ recommends using a **virtual private network** (VPN). A VPN can hide otherwise exposed devices and services on your network from an attacker's view while allowing you to authenticate and still access them remotely. This can reduce your attack surface significantly.[6]

  Attackers will only see the VPN instead of devices exposed to the internet.

- **Segment your network[7] to stop - internet-exposed services from reaching your internal network**.
  If your more vulnerable services get compromised, a segmented network will make it harder for attackers to reach other devices.

- **Patch[8] services and devices exposed on the internet.** Having the latest version will fix many of the vulnerabilities known to the vendor, and that means attackers have fewer known vulnerabilities they can use to gain access.

- **Turn on Multi-Factor Authentication (MFA)[9]** to add an extra layer of security and help prevent unauthorised access.

- **Use logging and alerting[10]** to help monitor devices and services, especially any that may be exposed on the internet. These are potential weak points that attackers may target. This can help notify you of an incident and provide details of what has happened.

Commonly targeted - internet-exposed services are:

- **NAS devices**
- **RDP**
- **Databases**
- **Device and service management interfaces**
- **IoT devices**

[4]https://www.cert.govt.nz/it-specialists/critical-controls/asset-lifecycle-management/
[5]https://www.cert.govt.nz/it-specialists/guides/unused-services-and-protocols/disabling-unnecessary-services-and-protocols/
[6]https://www.cert.govt.nz/business/ guides/securing-your-internet-exposed-rdp-server/
[7]https://www.cert.govt.nz/it-specialists/critical-controls/network-segmentation-and-separation/
[8]https://www.cert.govt.nz/it-specialists/critical-controls/patching/
[9]https://www.cert.govt.nz/it-specialists/critical-controls/multi-factor-authentication/
[10]https://www.cert.govt.nz/it-specialists/critical-controls/centralised-logging/

UPDATES

CERT NZ helps global open-source community with upgrade of Samba

In quarter two, a collaboration between CERT NZ, Catalyst and the open-source community has created a major update for Samba, making it more secure.

Samba enables Linux/Unix operating systems to communicate, share files, print and authenticate users with the Windows operating systems. Samba is used in many networks across New Zealand and the world.

This update improves the security of authentication within Samba, making it harder for attackers to gain access or information that they shouldn't have.

The update to Samba means the software is now more secure for users and as Samba is free and open-source, this provides benefits for users in New Zealand and the world.

The new upgrade brings Samba closer to Windows compatibility and allows the system to be updated more easily. As Catalyst's team works closely with Microsoft, the impact of the CERT NZ funding goes wider than the open-source community.

CERT NZ wants to acknowledge work done by the wider Samba community and thanks them for giving feedback. We appreciate all the effort involved.

Samba is freely available under the GNU General Public License.

Nudging for a more cyber secure New Zealand

Many New Zealanders put online security actions in the too hard basket, which exposes them to risk.

That's why CERT NZ has teamed up with The Research Agency to produce *Cyber Change* – a book of behaviour change techniques specifically aimed at prompting positive cyber security actions.

The book uses established behavioural science approaches and recent research on New Zealanders' online security attitudes to nudge them towards actions like updating devices and using stronger passwords.

The guide is for government and industry agencies who are working in the area of online security, and its purpose is to share insights about how to improve the effectiveness of cyber security interventions.

Cyber Change: Behavioural insights for being secure online is available at **CERT.govt.nz**

International insights

In this section, we cover news from our international partners.

EMOTET resurgence targeting credit card details

JPCERT (Japan) have noted an increase in Emotet malware reports since November 2021, spiking in February 2022, with over 1,200 incidents. This number closely reflects the initial spike in 2020.

A number of media outlets are reporting that the recent Emotet infections include a new module targeting Chrome browsers and scraping users' saved credit card details.

Alert Regarding Re-emergence of Emotet Malware Infection Activities

Traffic Light Protocol ratings updated

The Traffic Light Protocol (TLP) is a set of designations used to make sure that sensitive information is shared with the correct audience. In June, FIRST released a new version of the TLP ratings.

Authoritative from 5 August 2022, TLP version 2.0 includes the change of TLP:WHITE to TLP:CLEAR, and an additional TLP:AMBER rating, TLP:AMBER+STRICT which restricts sharing to the recipient's organisation only.

For more information, visit Traffic Light Protocol (TLP)