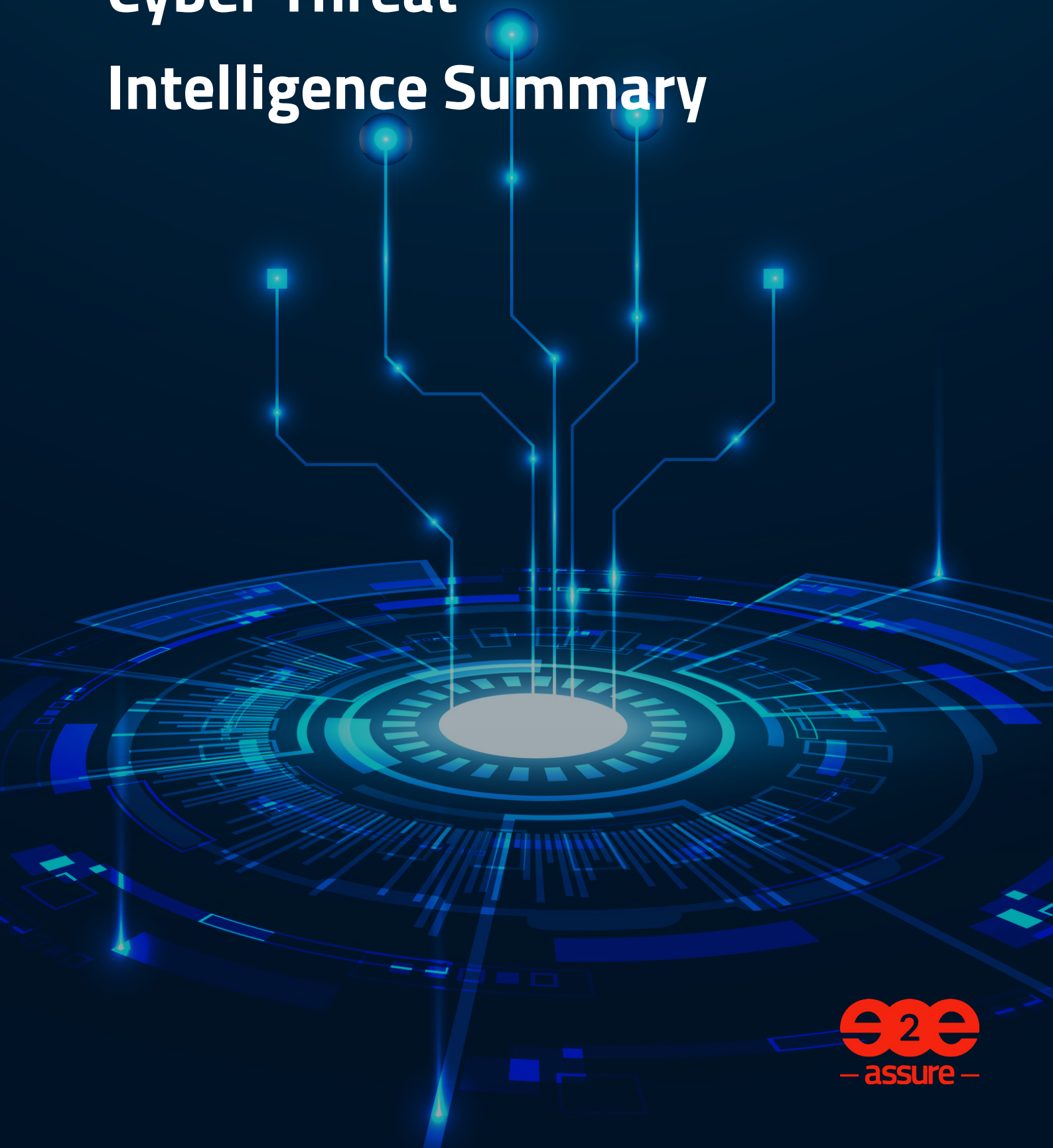


September 2023

Cyber Threat Intelligence Summary



Contents

1	BREAKING – ‘BLASTPASS’	03
2	UKUSA Alliance takes aim at Ransomware operators	04
3	...and Qakbot	05
4	Great news for the UK’s NCSC	06
5	Microsoft tracks new threat actor targeting Taiwan	10
6	UK MOD supplier attacked by LockBit	06
7	In brief!	06
8	Deep Dive – The Lazarus Group	06
9	Summary	06

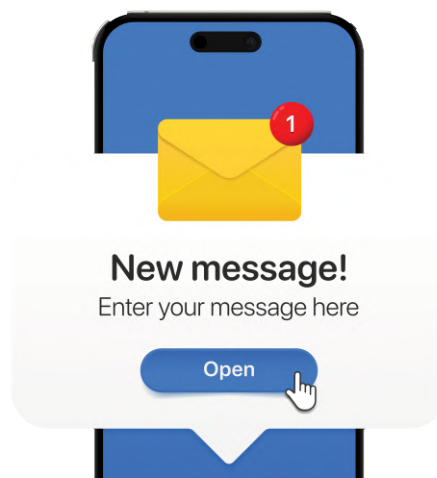
Welcome to our September edition of e2e-assure's threat intelligence briefing. With the cyber apprentices safely back in the classroom and Christmas cards already vying for space among the Halloween wares, we look at some of the events that happened in the ether while we were enjoying the balmy, summer.. downpours.

In response to some great feedback from you, our discerning reader, we've changed the format this month to bring you more actionable content at the marginal cost of a small drop in insight. Working on the premise of 'less is more' you told us that you found high-level, linked articles more useful with the occasional opinion piece and deep-dive still featuring. We listened and will continue to do so, please send your comments and opinions to us at cti@e2e-assure.com We hope you enjoy this edition!

BREAKING – 'BLASTPASS'

We've seen reports in the past week of a critical-level vulnerability in Apple's iOS/iPadOS, MacOS Ventura and WatchOS operating systems. Dubbed **BLASTPASS** and actually an exploit chain of a buffer overflow and a validation issue, this allows an attacker complete control over a device and requires zero interaction from the user. The infection vector is via a malicious iMessage and has been observed in the wild to deliver NSO Group's Pegasus spyware to victims.

Discovered by [The Citizen Lab](#) at The University of Toronto's Munk School in collaboration with Apple, this vulnerability affects the latest OS versions (16.6 in the case of iOS) on all iPhones from model '8' and later, all models of iPad Pro and MacOS Ventura, among others. These are being tracked as **CVE-2023-41064** and **CVE-2023-41061**.



Apple's [security team](#) have been quick to release patches for all products which perhaps gives an indication of the gravity with which this is being treated. The official advice is to **patch immediately** or place the device into Lockdown mode if you're unable to do so. Here are the links for [iOS/iPadOS](#) and [Mac Ventura](#).

Further information is not yet available, but we expect The Citizen Lab will publish a detailed breakdown on the exploit chain in the near future.



Source: [bleepingcomputer.com](#)

UKUSA Alliance takes aim at Ransomware operators

In a co-ordinated assault on cyber-crime, the UK's Foreign Office and the USA's DoJ have created a series of sanctions against eleven members of the infamous 'Conti/Trickbot' gangs. Following a complex investigation by the UK's National Crime Agency (NCA) it was assessed that the group were responsible for the extortion of at least £27 Million from 149 UK individuals, businesses and institutional targets, including schools, hospitals and local government organisations. The sanctions centre around the freezing of assets and impose travel restrictions on the eleven Russian nationals, although it remains to be seen how much impact these will have, beyond raising awareness of the individuals themselves.



UK Deputy PM Oliver Dowden has been quoted:

“By targeting these malicious cyber actors, who have been known to work with some of the most damaging ransomware strains, we are seeking out and exposing those who threaten the UK's national security. We will always take decisive action with international partners to protect the UK, its people and businesses.”

<https://www.gov.uk/government/news/uk-sanctions-members-of-russian-cybercrime-gang>



...and Qakbot

Those sanctions came hot on the heels of another UKUSA co-operation, this time led by the DoJ and involving action across the United States, UK, France, Germany, the Netherlands and some Eastern European states in a notable offensive cyber operation to 'seek & destroy' the Qakbot infrastructures. Attorney General Merrick B. Garland said:

“Together with our international partners, the Justice Department has hacked Qakbot's infrastructure, launched an aggressive campaign to uninstall the malware from victim computers in the United States and around the world, and seized \$8.6 million in extorted funds.”

Qakbot, aka 'Qbot' or less frequently 'Pinksliptbot' is an initial access and persistence mechanism widely used by groups such as Conti, REvil & Black Basta, delivered via the execution of a malicious email attachment or link. Infected machines become part of a Botnet under the control of the threat actor, with the user typically unaware.

In May's edition we highlighted the useful service provided by the Dutch Police to check email addresses against those discovered to be victims in the Genesis Market takedown. The scope of this service has been widened to include victims of Qakbot and can be found here:

<https://www.politie.nl/en/information/checkyourhack.html>

The US Department of Justice has also supplied the same dataset to the popular [HavelBeenPwned](#) website. If you're a victim of a Ransomware attack, this should be reported to the NCSC's [Cyber Incident Service](#) in the UK, followed by a call with our DFIR specialists at e2e-assure. We can help you to respond, manage and recover and rebuild stronger for the future.

<https://www.justice.gov/opa/pr/qakbot-malware-disrupted-international-cyber-takedown>



Great news for the UK's NCSC



Ollie Whitehouse
Chief Technology Officer



Source: twitter.com/NCSC

Remaining on a Government topic, we at e2e-assure were delighted to learn that industry stalwart and cyber security expert Ollie Whitehouse has been appointed CTO of the National Cyber Security Centre. Starting in October of this year, Ollie will “will play an instrumental role in shaping and delivering the UK’s national approach to cyber security.” Ollie, a near thirty-year veteran of the industry was quoted on the NCSC website as saying:

“I’m honoured to be starting as Chief Technology Officer at the NCSC and look forward to supporting its world-class talent in their critical work keeping the UK safe online.”

Congratulations Ollie, we wish you every success in your role and look forward to working alongside you!

<https://www.ncsc.gov.uk/news/ollie-whitehouse-new-ncsc-cto>

Microsoft tracks new threat actor targeting Taiwan

At the end of August, Microsoft released an interesting and highly detailed threat brief around a campaign the vendor has uncovered by a threat actor it is naming 'FLAX TYPHOON' giving it a classification that Microsoft attributes to being aligned with China.

As we've covered in previous editions of this briefing, LOLBins is the process by which a threat actor will leverage legitimate tools and operating system components on the victim machines in order to achieve their objectives. Because the reliance on detectable malware



Redmond have witnessed attempts to gain access to multiple Taiwanese organisations, with the assumed intention of conducting espionage activities. What makes this group interesting and potentially harder to detect, is their preference for the use of living-off-the-land binaries, aka LOLBins.

is reduced this naturally removes that detection vector. This is not exclusive however and in addition to this practice, the group have been observed to deploy known malware such as 'China Chopper', 'Juicy Potato' and 'BadPotato' among others.

We recommend you take the time to read through the full article which is linked below, if you're pushed for time here is a key takeaway in the form of a Sentinel hunting query that you can use to detect FLAX TYPHOON activity in your network:



```
let ipAddressTimes = datatable(ip: string, startDate: datetime, endDate: datetime)
[
    "101.33.205.106", datetime("2022-11-07"), datetime("2022-11-08"),
    "39.98.208.61", datetime("2023-07-28"), datetime("2023-08-12"),
    "45.195.149.224", datetime("2023-01-04"), datetime("2023-03-29"),
    "122.10.89.230", datetime("2023-01-12"), datetime("2023-01-13"),
    "45.204.1.248", datetime("2023-02-23"), datetime("2023-05-09"),
    "45.204.1.247", datetime("2023-07-24"), datetime("2023-08-10"),
    "45.88.192.118", datetime("2022-11-07"), datetime("2022-11-08"),
    "154.19.187.92", datetime("2022-12-01"), datetime("2022-12-02"),
    "134.122.188.20", datetime("2023-06-13"), datetime("2023-06-20"),
    "104.238.149.146", datetime("2023-07-13"), datetime("2023-07-14"),
    "139.180.158.51", datetime("2022-08-30"), datetime("2023-07-27"),
    "137.220.36.87", datetime("2023-02-23"), datetime("2023-08-04"),
    "192.253.235.107", datetime("2023-06-06"), datetime("2023-06-07")
];

let RemoteIPFiltered = DeviceNetworkEvents
| join kind=inner (ipAddressTimes) on $left.RemoteIP == $right.ip
| where Timestamp between (startDate .. endDate);

let LocalIPFiltered = DeviceNetworkEvents
| join kind=inner (ipAddressTimes) on $left.LocalIP == $right.ip
| where Timestamp between (startDate .. endDate);

union RemoteIPFiltered, LocalIPFiltered
```

<https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/>

UK MOD supplier attacked by LockBit

In an effort to dispel headlines which are in our opinion approaching 'FUD', the UK MOD has not been breached by LockBit. On 5 August, UK security fencing manufacturer Zaun suffered an intrusion on a vulnerable (Windows 7) machine in their manufacturing process, in which the attacker exfiltrated around 10GB of data. Contained within this dataset were allegedly plans and drawings relating to key, military installations around the UK, including RAF Waddington, home of the UK's Reaper drone fleet and HMNB Clyde at Faslane, home to our nuclear submarine fleet.

Zaun invoked its contingency plans and are working with the West Midlands RCCU and the NCSC to contain the breach and assess the impact. While the company states that they believe no classified material has been lost, clearly this is a serious incident that has the potential to impact the security of UK military installations, at least in the short-term.

Defence Chair and MP Tobias Ellwood has asked the question:

“

How does this affect the ability of our defence establishments to continue functioning without threat of attack? How do we better defend ourselves from Russian-backed interference no doubt related to our stance in supporting Ukraine?

”



You can read Zaun's statement [here](#); we expected that there will be a strong 'lessons learned' exercise around this and will bring you updates as they unfold. Our initial take is that a vulnerable Windows 7 machine should have been isolated and air-gapped from any Internet-connected network!

<https://www.mirror.co.uk/news/uk-news/russia-linked-hackers-hit-uk-30850139>

In brief!

A round-up of the best of the rest, articles we used for research that didn't make the final cut but we feel are still worthy of a mention:

[Juniper warns users about denial-of-service bugs in JunOS](#)

[Netgear releases patches for CVE-2023-41182&3 present in its NMS software](#)

[The Guardian becomes latest media outlet to block ChatGPT](#)

[Cloud Security firm AquaSec exposes vulnerabilities in MS PowerShell repo](#)

[UK Parliamentary researcher arrested on China spying charges](#)

[Google releases 'Quantum-resistant' security keys](#)

Deep Dive

The Lazarus Group



A notorious and high-capability threat actor strongly associated with North Korea, our look at Lazarus aka 'HIDDEN COBRA' and APT38 focuses on its inception and past activities while considering what may be their next steps.

In the world of cyber espionage and criminal activities, few groups have gained as much notoriety as the Lazarus Group. This shadowy collective of hackers has been implicated in a range of high-profile cyberattacks, leaving a trail of disruption, theft, and geopolitical tension in its wake. We delve into the history, motivations, and future potential of the Lazarus Group, shedding light on its operations and impact on the global cybersecurity landscape.

The group made its first appearance on the radar of cyber security experts in the late 2000s. Thought to be based in North Korea, the group's origins are shrouded in mystery, although early reports suggest that the group might have been formed as a specialised unit within North Korea's Reconnaissance General Bureau (RGB), tasked with conducting cyber operations to further that regime's goals.

While the identities of its founding members remain undisclosed, cybersecurity analysts have attributed various cyber campaigns to the Lazarus Group based on distinct TTPs. Its operations have ranged from financial theft to political disruption, pointing towards a multifaceted and adaptable threat actor. Motivations are complex and appear to align closely with North Korean state interests. Its activities often reflect a blend of political, financial, and ideological objectives. Notably, the group has been linked to several high-profile attacks that have garnered international attention and condemnation.

One of its most notorious campaigns was the 2014 Sony Pictures hack, which exposed sensitive corporate data, embarrassing emails, and resulted in the cancellation of the film "The Interview." The attack was believed to be retaliation for the movie's portrayal of North Korean leader Kim Jong-un. In 2016, the group was linked to the cyber heist targeting the Bangladesh Central Bank, where hackers stole over \$81 million. The group's involvement was revealed through the distinctive malware used in the attack. Victims also include cryptocurrency exchanges, such as the high-profile breach of the Japanese exchange Coincheck in 2018, where hundreds of millions of dollars' worth of cryptocurrencies were stolen.

As the cyber security landscape evolves, so too does the Lazarus Group's potential for disruption. Its ability to adapt its tactics and targets suggests an ongoing willingness to exploit emerging vulnerabilities. With the proliferation of interconnected devices and critical infrastructure, the group may seek to exploit new avenues for espionage and financial gain.



Western governments have been quick to denounce the Lazarus Group's actions and attribute its activities to North Korea. Statements from notable figures reflect the concerns surrounding the group's actions and its implications for international security. Former U.S. National Security Advisor, John Smith, emphasized the need for a united front against cyber threats, stating:

“The Lazarus Group's actions underscore the urgency for a coordinated response to counter the growing menace of state-sponsored cyber operations. We must remain vigilant and resilient in the face of these evolving threats.”

The Lazarus Group's presence in the cyber realm continues to perplex and alarm experts worldwide. Its history of audacious attacks, political affiliations, and evolving tactics paint a picture of a group that is as adaptable as it is dangerous. As technology advances and new vulnerabilities emerge, it is imperative for governments, cybersecurity professionals, and the private sector to collaborate and defend against this persistent threat. Only through collective efforts can the world hope to mitigate the impact of groups like the Lazarus Group and safeguard the digital future.

For further reading, we recommend Cisco's Talos group [report](#) as a great starting point.



Let's connect!

That's it for this edition of e2e-assure's CTI briefing, we hope you've enjoyed the content and we welcome any feedback you have at cti@e2e-assure.com