DNSFilter

BEYOND HACKERS IN HOODIES:

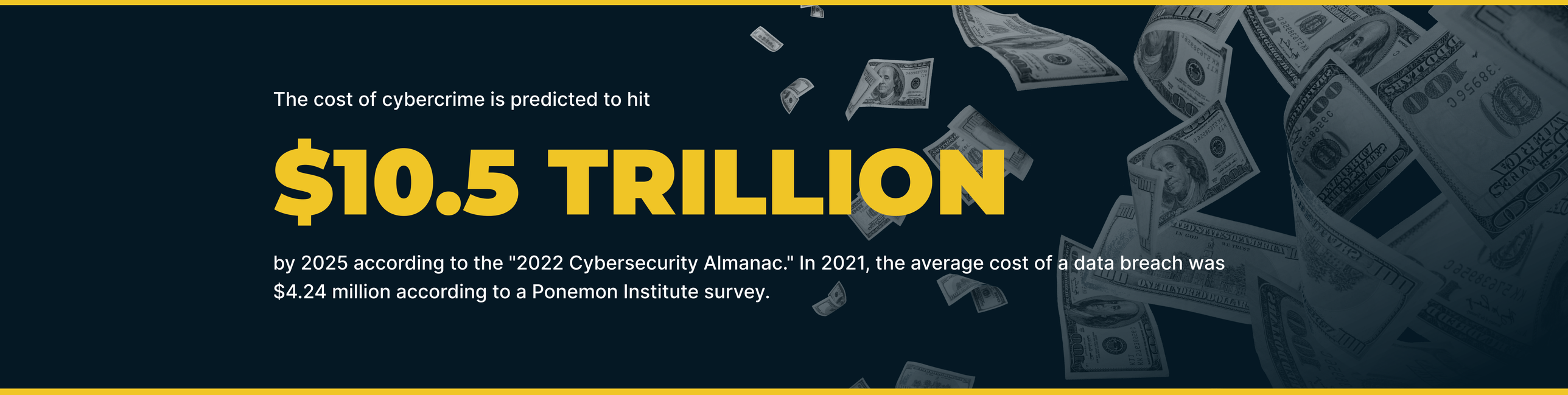
DNSFILTER MID-YEAR CYBERSECURITY REVIEW

FULL REPORT

THREATS BY THE NUMBERS

82% of those surveyed by VMWare say they're concerned that their company is vulnerable to a cyber attack.

49% of respondents think their organizations lack expertise and tools to adequately handle an attack.



The cost of cybercrime is predicted to hit

$10.5 TRILLION

by 2025 according to the "2022 Cybersecurity Almanac." In 2021, the average cost of a data breach was $4.24 million according to a Ponemon Institute survey.

Of data breaches in 2021, healthcare industry breaches were the costliest—

$9.23 MILLION

on average.

On the DNSFilter network, we noticed a

218%

increase in traffic to malicious sites with "health" in the domain name in April of 2022.

36%

of data breaches involve phishing, per Verizon's annual Data Breach Investigations Report.

90%

of cyber attacks begin as spear phishing emails according to Trend Micro.

At the end of 2021 through the end of the year, we saw a

300%

increase in phishing traffic on our network.

THE TRENDS ARE IN THE

DNS

THE DNSFILTER NETWORK IS A MIRROR TO REALITY

Since the release of our October 2021 Threat report, we have continued to stay on top of interesting threat patterns observed on our network. This has helped us detect growing threat concerns and communicate them to our users accordingly.

In this report, we'll take a look at network activity at DNSFilter and correlate our findings with events in the news.

DDOS AND BOTNET

BOTNET TRAFFIC PATTERN FROM MARCH 2021 TO MARCH 2022

At the end of December 2021 and early January 2022, we started to observe higher activity of Botnet traffic on our network. Within this period, we observed a 171% increase in Botnet traffic compared to the highest peak during the entirety of 2021. Though this was unusual compared to how the traffic had looked prior to that time, the intensity was not so concerning and it eventually dipped towards the end of January.

However, when February rolled around we saw spikes in order of magnitudes higher than the ones experienced in January. Botnet traffic during this time saw a 1200% increase compared to the highest daily spike in 2021. This increase in Botnet traffic remained consistent throughout the month of February.

This was around the same time the **BBC reported** that European oil facilities were being hit with a wave of cyberattacks. A notable victim was Oiltanking Germany whose IT services were disrupted, affecting every port they operated in Europe and Africa. Experts say this might have been a ransomware attack.

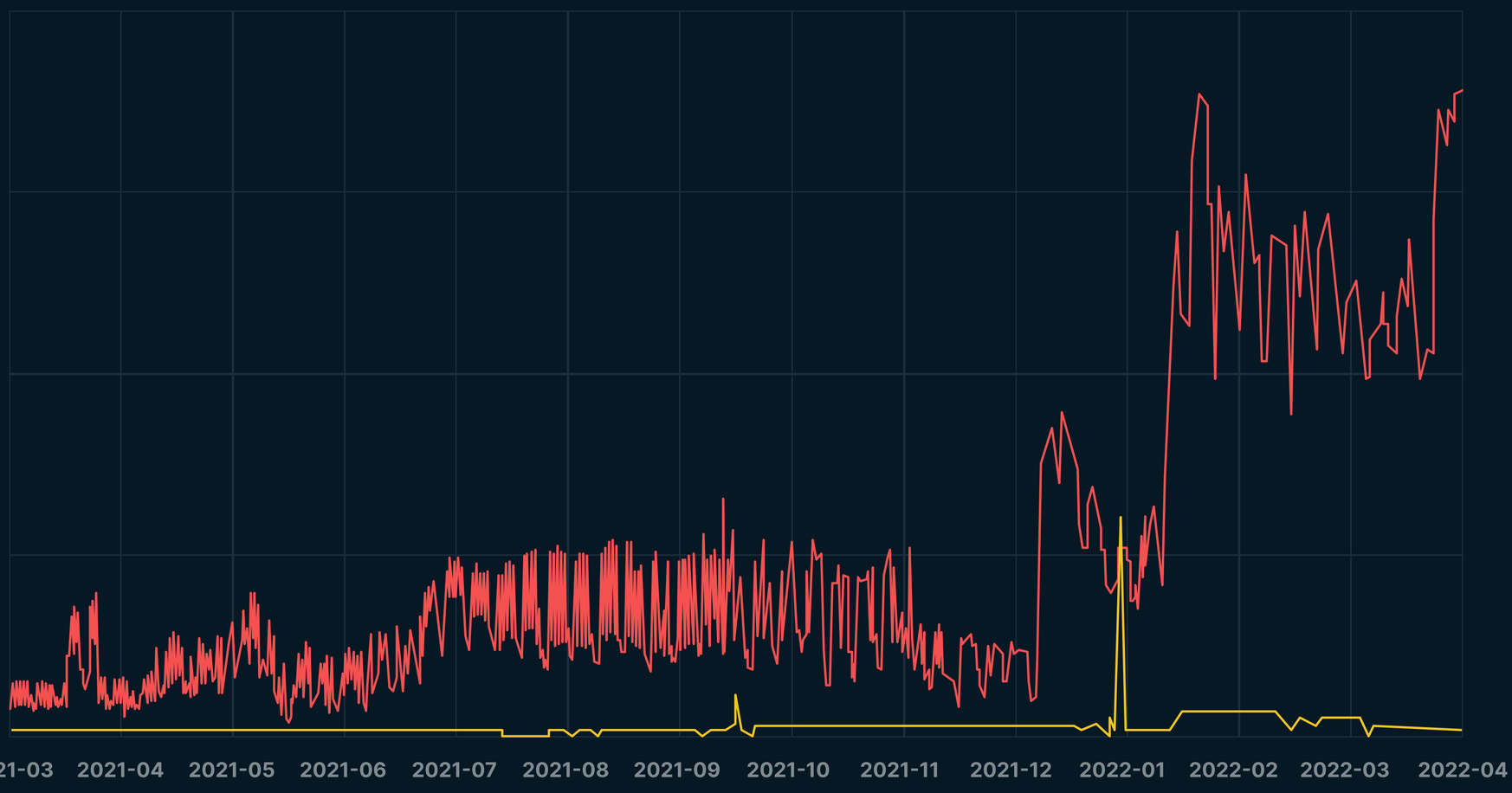
171% INCREASE IN BOTNET TRAFFIC

1200% INCREASE INCREASE COMPARED TO THE HIGHEST DAILY SPIKE IN 2021

Another event that was reported around this period was the **DDoS attacks on multiple Ukrainian banks and government departments' websites**. The attack began on Wednesday the 23rd of February, just a day before Russia launched military actions on Ukrainian soil, **when internet connectivity company NetBlocks tweeted about the outages**, saying "the incident appears consistent with recent DDoS attacks".

On our network, the majority of our botnet traffic stemmed from sites related to cryptocurrency. We couldn't identify any trends to Russia or Ukraine—though we did find one major botnet site that was registered in Germany. We'll cover traffic to crypto-related sites on our network later.

MALWARE



MALWARE TRAFFIC PATTERN FROM MARCH 2021 TO MARCH 2022

Malware is a very active threat category on our network, thus, it takes a very chaotic and extreme malware pattern for us to begin to suspect that something special might be happening.

This was the type of pattern we started to see around mid-January, 2022. The malware levels rose over 200%. Though our AI continued to block these threats, multiple spikes were continuously observed going into the month of March. These spikes persisted throughout the month of April at a 100% average increase from the traffic observed before mid-January.

Around this time, news about **the Wiper malware** affecting multiple Ukrainian computers was already making headlines.

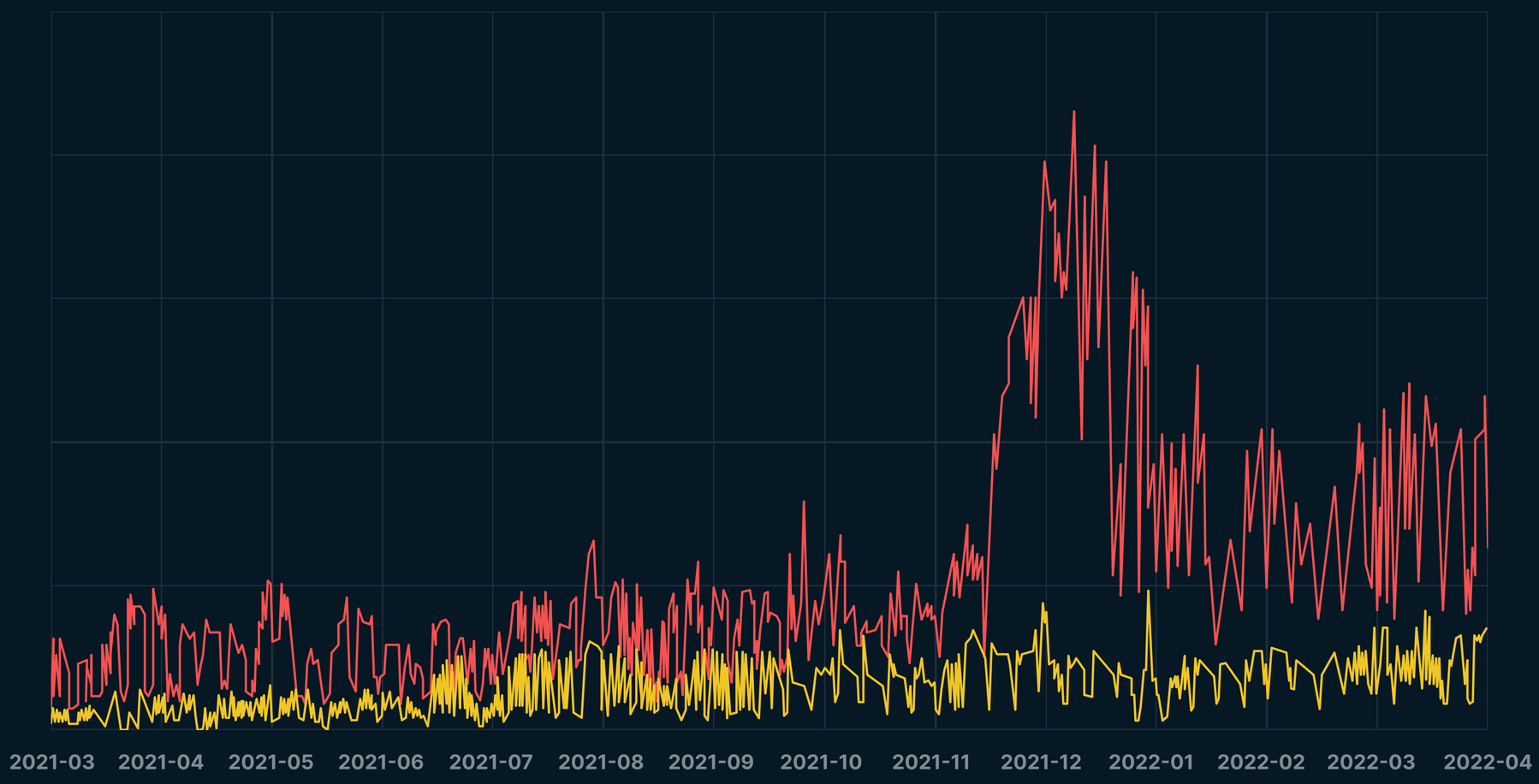
Prior to that, **Microsoft had put out a report** stating it had discovered malware on dozens of Ukrainian government computers that could prove more destructive than the company originally thought. This report coincides with the attack that took down 70 Ukrainian government websites.

In a research report published by the National Cyber Security Centre in the UK and US agencies including the National Security Agency, the agencies warned that a Russian state-backed hacker group known as Sandworm had developed a new type of malware called Cyclops Blink. This malware targets firewall devices made by the manufacturer Watchguard to protect computers against hacks.

This Cyclops Blink malware was reported to be so resilient that it could withstand typical remediation attempts like system reboots. The research, however, was done as routine advisory efforts and not at all linked to the Russian-Ukraine crisis.

Around this time, the average number of domain names with the words “**blink**” and “**cyclops**” observed on our network rose from 58.5k to 93.5k daily representing a 60% increase compared to the last half of 2021.

PHISHING AND DECEPTION



PHISHING AND DECEPTION TRAFFIC PATTERN FROM MARCH 2021 TO MARCH 2022

Similar to Malware, Phishing is another threat category where the city never sleeps. Most often used as a conduit for deploying malware, phishing has proven to be an effective strategy for tricking victims into taking actions that allows threat actors to compromise computer systems and networks.

Up until November, the phishing traffic on our network had been fairly regular. A sudden surge as high as 300% compared to the previous average traffic was then noticed around November 13, 2021, and persisted till the end of the year.

This observation coincided with threat actors **compromising internal Microsoft Exchange servers** using the **ProxyShell** and **ProxyLogon** vulnerabilities to perform phishing attacks. Once they gained access to a server, they used the internal Microsoft Exchange servers to perform reply-chain attacks against employees using stolen corporate emails.

One of the biggest victims was retail giant, IKEA. Threat actors used this vulnerability to target IKEA employees in an internal phishing attack using stolen reply-chain emails. Reply-chain emails are very dangerous because they are legitimate emails from a company and are commonly sent from compromised email accounts and internal servers. Thus, recipients will trust the email and be more likely to open the malicious documents.

In response to this attack, IKEA IT teams sent out an internal email to warn employees of an ongoing reply-chain phishing cyberattack targeting internal mailboxes. These emails were also being sent from other compromised IKEA organizations and business partners.

The internal email also stated that these reply-chain emails contain links with seven digits at the end and employees were told not to open the emails, regardless of who sent them, and to report them to the IT department immediately.

During the period of this attack, an 88% increase in the number of phishing URLs containing the keyword "**ikea**" was detected on our network.

Another notable company that was hard hit by this wave of phishing attacks was Godaddy. Godaddy's Chief Information Security Officer on Nov. 17, 2021, disclosed that **suspicious activity was discovered** in the company's managed WordPress environment, which turned out to be a third-party using a compromised password to gain access. Up to 1.2 million active and inactive Managed WordPress customers had their email addresses and customer numbers exposed.

Godaddy responded by resetting the WordPress account and database passwords of affected customers and also issuing new SSL certificates. However, the exposed emails continued to pose a great risk of impending phishing attacks.

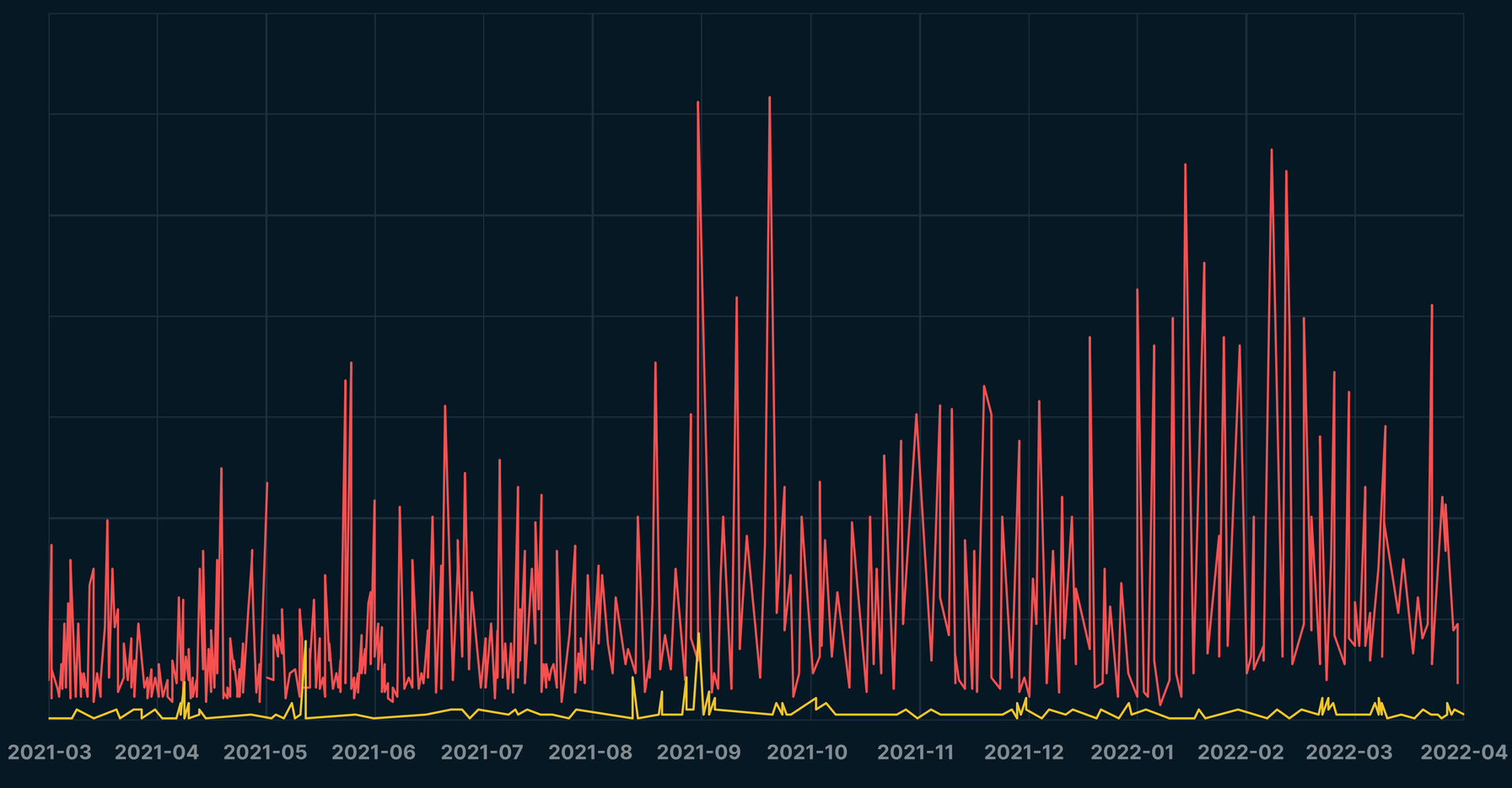
By the 24th of November, this hack that exposed millions of emails had **spread to six (6) more web hosts**.

In the world of cryptocurrency, a hacker was able to steal more than fifty-five million dollars ($55m) after a bZx developer fell for a phishing attack. This attack, which was reported by Business Insider on the 7th of November 2021, further shows how potent phishing attacks can be.

88% INCREASE IN THE NUMBER OF PHISHING URLS CONTAINING THE KEYWORD "IKEA"

A HACKER WAS ABLE TO STEAL MORE THAN FIFTY-FIVE MILLION DOLLARS ($55M)

P2P & ILLEGAL



PEER-TO-PEER AND ILLEGAL TRAFFIC PATTERN FROM MARCH 2021 TO MARCH 2022

Unlike in previous years, Peer-to-Peer traffic stayed busy since March 2021 and has remained so to date with spikes occurring at close intervals. Based on our research on the network, business, and social activities involving illegal peer-to-peer communication, we have come up with a theory on why these traffic patterns emerged: The rise of cryptocurrency.

Since 2020, the year the world was locked down, we have witnessed a huge increase in cryptocurrency interest. The surge in the prices of Bitcoin and many altcoins led to rapidly growing interest in possessing and trading crypto money as indicated below by this Google trends chart for the word "**crypto**" from June 2020 to December 2021.

GOOGLE TRENDS FOR THE WORD "CRYPTO" FROM JUNE 2020 TO DECEMBER 2021

More crypto activities led to more mining operations and fraudulent transactions. Coupled with the many reservations about crypto and its environmental consequences, national governments started looking into controlling crypto activities.

While some governments sought to create policies and regulations to "tame the beast", other governments weren't so accommodating. The governments of **China**, **India**, **Nigeria**, and **others** banned cryptocurrency activities declaring them illegal. Defaulters had their bank accounts frozen and were sometimes arrested. Any financial institution involved in cryptocurrency transactions was either fined or had their license revoked.

Because these governments relied on centralized systems to track cryptocurrency activities and their participants, traders in these countries began to move to peer-to-peer systems to continue trading. This allowed cryptocurrency activities to continue to experience a rise despite the government bans.

With this safe trading medium came the inevitable ugliness of scams and illegal transactions. We believe that the persistently busy peer-to-peer illegal traffic witnessed on our network over the past year can be attributed to the growing use of peer-to-peer mediums for trading cryptocurrencies.

RUSSIA'S HYBRID WAR:
HOW THE WAR ON UKRAINE STARTED LONG BEFORE MILITARY ACTION

We are all aware of the ongoing war on Ukraine by Russia with the first military assault made by Russia on the 24th of February, 2022 when a series of explosions were first reported in Kyiv, Kharkiv, Odessa, and the Donbas. However, what many might not know is that this war may have started long before the February 24th event.

According to ABC news, in mid-January Wiper malware was spreading quickly and led to the defacement of up to 70 Ukrainian government websites. This attack was also used to penetrate Ukrainian government networks.

Therefore, it didn't come as a surprise to the Ukrainian government and cybersecurity experts when Ukraine was hit with a wave of Distributed Denial of Service (DDoS) attacks a few hours before the military assault began. According to cybersecurity researchers, hundreds of computers were also infected with destructive malware. Some of the targets include Ukraine's defense and foreign ministries, the Council of Ministers, and Privatbank, the country's largest commercial bank.

It was earlier reported that many of the sites were similarly knocked offline between Feb. 13-14 in DDoS attacks, prior to the commencement of military attacks on Ukraine on Feb 24th. An attack the U.S and U.K blamed on Russia's GRU military intelligence agency.

This hybrid form of warfare, which involves combining cyberattacks with military onslaughts, is a typical pattern of the Russian government when attacking another nation.

Russia had previously used this type of hybrid warfare tactics when it hit **Georgia** and **Crimea** with multiple DDoS attacks during the incursions in **2008** and **2014** respectively.

According to BBC, the timeline of cyberattacks showed that Ukraine first experienced a wave of DDoS attacks on Wednesday, a few hours before the launch of military action on Thursday, February 24th, 2022. The same night on Wednesday, cybersecurity experts at Symantec and ESET reported that a second form of attack, this time malware, had hit multiple Ukrainian computers. ESET telemetry shows that the malware was installed on hundreds of machines in the country.

From timestamps obtained from the malware, it was discovered that "**Wiper**" malware had been installed on the 28th of December, 2021. This gives a rough estimate of how long the cyberwar on Ukraine had started before the missiles hit.

BBC, through a researcher, gathered that the Ukrainian military and banking websites were able to recover rapidly due to preparedness and increased capacity to implement mitigations. This further emphasizes the need for organizations to employ a proactive approach when it comes to combating cyber threats.

DISGUISED THREATS:
HOW ATTACKERS ARE MAKING YOU FOCUS ON THE WRONG PROBLEM

From the 1995 movie “The Usual Suspects” came what will go down as one of the most memorable quotes in TV history and it goes thus:

> **THE GREATEST TRICK THE DEVIL EVER PULLED WAS CONVINCING THE WORLD THAT HE DIDN’T EXIST**

The quote, which is a paraphrased version of a quote by the French poet Charles Baudelaire, describes a diversion technique used by an ill-intentioned actor to conceal their actual malicious purpose by deceiving the victim with a smokescreen.

From our observations of recent cyberattacks, It seems that threat actors are now making use of this technique to send threat victims and experts trying to fix the problem on what can best be described as a “cyber wild goose chase”, while the attacker perpetrates a more nefarious act or covers a larger attack surface.

These diversion techniques are a luxury for attacks involving Advanced Persistent Threats (APTs) as they help buy more time for the attack operation even after detection. A data exfiltration attack can be masked as ransomware causing the victims to waste time negotiating a ransom while sensitive data is continuously mined.

For example, the **Wiper malware attack** that was used to intrude into Ukrainian government networks by the Russians was disguised as ransomware while the worm spread. This diversion led to the damage of two Ukrainian servers before it was detected and stopped.

The **malware reported by Microsoft** on January 16, 2022, was disguised as a blackmail program. Meanwhile, its true intent was to destroy data at the hacker’s command.

If this continues to be a lucrative pattern for threat actors, the need for more intelligent threat detection tools cannot be over-emphasized. IBM stated in its **2021 Cost of a Data Breach report** that Automation and security artificial intelligence (AI), when fully deployed, provided the biggest cost mitigation, up to USD $3.81 million less than organizations without it.

These tools, like DNSFilter’s AI-based categorization, have the ability to feed on historical threat data to discover threat patterns and can be continuously tuned to accurately predict threat types.

DNSFilter

GET DNS SECURITY

DNSFilter is an AI-powered threat protection and content filtering service that provides a **secure gateway for all your DNS traffic**. DNSFilter accurately predicts malicious and inappropriate sites and blocks them from your network. We are backed by the largest global DNS network in the industry and can be deployed to start filtering your web traffic in a matter of minutes.

SCHEDULE A MEETING WITH ONE OF OUR TECHNICAL EXPERTS.

BOOK A DEMO