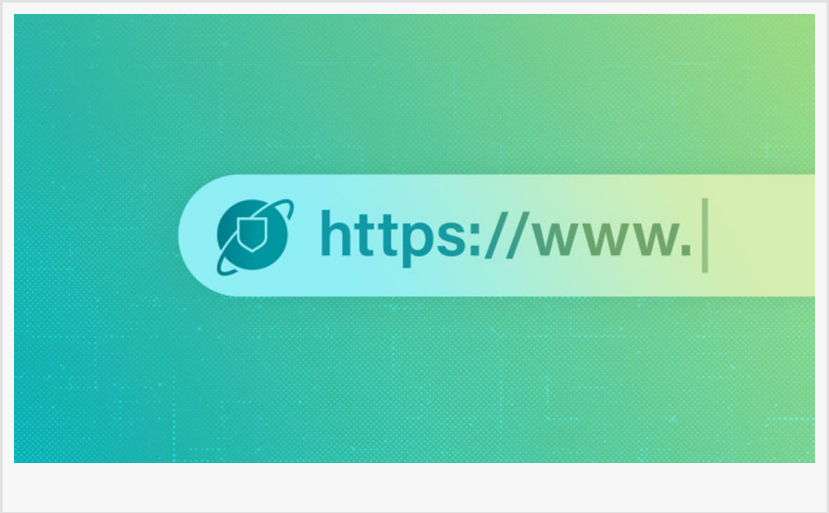
Delivering trust with DNS security



DUBAI , DUBAI, UNITED ARAB EMIRATES, January 10, 2024 /EINPresswire.com/ -- Alžbeta Kovaľová, writer at ESET, discusses whether DNS protection technology can transform consumers' worries about cybercrime with a trust-based approach.

Cybercrime continues to grow rapidly; indeed, it is a highly lucrative global industry. Without accurately accounting for profits from cybercrime, we are left looking at the staggering estimated cost of US$7.08 trillion in 2022 for reference. Measured in terms of GDP, the illegal proceeds would rank as the third-largest "economy" worldwide. Regardless, this landscape keeps evolving, driven by new tech, further monetization of the internet, new illicit opportunities enabled by the vibrant cybercrime as-a-service business model, and ever more resources invested in criminal profit extraction.

Cybercrime has global reach, knows no borders and the barrier to entry is low. Indeed, compared to traditional crime, this is a high-reward, low-risk 'enterprise', with law enforcement facing persistent challenges in bringing cybercriminals to justice. Its growth is further fueled by the fact that many people aren't prepared to face digital threats. Lastly, the opportunities to pursue cybercrime loom large over both consumers and business 24/7 and can impact nearly every person or organization that has or handles personal or otherwise valuable data.

Due to the scale of the problem and the surge in its impacts, consumers are becoming increasingly concerned about their online safety and privacy, prompting a demand for greater protection under the law and transparency in data transmission, not only with sensitive services like finance, but also extending to transportation and even entertainment. Concern has also impacted consumers' "attitudes" regarding how their chosen digital security products and services function, and how those functions are implemented to further the continued growth in the cybersecurity industry. However, what these changes don't show is that many threats, especially web threats, still manage to slip through the cracks.

To address those threats, shifts in technology are needed that align with the everyday risk users

take when they have to share their personal data with websites and apps. This need goes beyond AV products that mainly protect investments made in PCs [which, coincidentally, require certain data collection to be able to analyze threats and recognize them in future instances (e.g., identification of types of malicious code attempting to infect a device)].

Instead, emerging approaches to protection need to deliver impactful security that mitigates web-based threats. This calls for security vendors and Internet Service Providers (ISPs) – in tandem – to focus on protecting trust itself. These efforts have led to the development of products and services that secure the precise moments a user takes action based on an (online) trust relationship. One powerful approach can be accomplished by blocking many methods prized by cybercriminals at their very foundations, namely at the Domain Name System (DNS) level.

Web threats

The size and scope of the world wide web mean that the true miracle of its inception is the ability to search, filter, and successfully access content. While DNS is actually a pairing of numeric Internet Protocol (IP) addresses used by computers with text-based domain names used by humans, for users it's an address book for the web and performs unnoticed.

However, times change. We can muse that threats and malicious domains should never have entered into existence, but the growing number and complexity of threats shows that to be an impossibility. Thus, DNS is increasingly looked at to provide comprehensive protection, a role it can play by filtering out malicious or suspicious domains. To create a workable DNS-level security solution, security vendors, ISPs, and telecommunications or communications service providers (TELCOs) have to partner up and deploy these automated systems at scale.

As almost all world wide web activity takes place through DNS, using it to tackle web threats is no small matter. Telemetry from ESET and other vendors shows that despite the fact that the number of potential web threats has gone down slightly in the past years, some, like phishing, continue to be prevalent. Statistics from the T3 2022 Threat Report showed that, for example, the total number of blocked phishing websites climbed to 13 million globally.

Newer developments seen with web threats involve legitimate websites hosting malware, called malware objects, which have been documented by ESET since its Q2 2022 Threat Report. Here, an otherwise legitimate website from a legitimate author has been compromised by a third party who has implanted malicious functions: weblinks, pdfs, or lead capture, or the website has become host to a service that allows others to store or download files. Those files could then include malicious code, illegal or harmful content, or malware objects.

IoT Threats

Internet of Things (IoT), another name for smart devices that work by being connected to the internet, include items like baby monitors, door cameras, TVs, medical devices, home appliances, network routers, and much more. Oftentimes, these gadgets have been rushed to market

without robust security measures in place and have limited to non-existent on-device security features, including weak authentication mechanisms, vulnerabilities and non-existent update paths, and unencrypted data transmissions. As a result, cybercriminals can misuse IoT devices broadly, including to create massive networks of compromised devices known as botnets. These can be used to overwhelm various types of online systems, from websites to telecommunications services and critical infrastructure.

Addressing IoT security is critical because botnets pose a significant threat, whether used to execute massive DDoS attacks, brute force (password/credential guessing), further infections, or vulnerability exploitation. They do this by compromising the network or the devices that have a cloud-based control panel (for example, old IP cameras) the IoT device is connected to. Since IoT devices are operated via connection to a router, many doors are open for those wanting to cause harm. Botnets are one of attackers' most prized tools, and one that DNS-level protection is highly effective against.

With significant incidents as early 2001, attacks have only increased in scale, regularly disrupting or even preventing access to some of the world's most popular websites and services. One of these, the Mirai botnet, has since 2016 periodically hijacked consumer-grade Internet of Things (IoT) devices, using hundreds of thousands of them to orchestrate attacks. These attacks can still be detected in 2023.

Other botnets, like Mozi, which have joined the threatscape more recently, have also benefited from variants of Mirai, that is until October 2023 when it virtually disappeared in an apparent takedown. During its reign between 2019 and 2023, the Mozi botnet became the largest of its kind, at one point incorporating over 1.5 million unique devices into its network and operating mainly through known vulnerabilities in NETGEAR DGN devices and JAWS web servers.

Routers

Joining IoT threats, web threats vectoring through compromised routers can be managed with DNS Security by blocking access to malicious or suspicious domains. This works to interrupt criminal infrastructure like phishing and malicious websites used to steal users' personal data and credentials. DNS security, paired with a multilayered security solution that features network inspection tools, which enable users to test their routers for weaknesses such as poor passwords and out-of-date firmware. This combination mitigates the security implications of technology's relentless march toward bringing all kinds of everyday physical objects online and making them "smart."

And, while smart is the new standard, we must recognize that many risks follow when "everyday objects" are embedded with software, processors, sensors, actuators, and internet connectivity that enable them to collect data and interact both with their environment and one another.

When discussing the myriad smart devices that now inhabit our homes, it's essential to put a spotlight on routers. Not only are these the unsung heroes of modern connectivity remaining

turned on 24/7, but they are actually the foundation of the connected home. In fact, they are specialized computers whose operating systems, embedded as firmware, require critical updates to address security loopholes, and are subject to manufacturer-maintained lists of end-of-life devices.

And, while routers don't store people's personal data, all traffic from every internet-enabled device in a household goes via the router. Poorly secured, they can put all devices on a network at the mercy of bad actors. And, in an era of remote/hybrid working, their security has taken on greater importance and may even have implications for corporate networks. Here a few measures go a long way: using strong passwords instead of defaults, applying the highest level of encryption, disabling remote management access and both unnecessary services and features to reduce attack surfaces, or creating separate networks for IoT devices to protect data on PCs and smartphones.

Keeping the world connected and secure

The TELCO and ISP industry, which profits from global connectivity, also bears the responsibility of safeguarding vast amounts of personal data entrusted to it by their customers. Properly managing this data is pivotal to TELCO and ISP reputation and ensuring the trust needed to fuel their business model.

In response to growing pressures from cybercriminals and the evolving needs of their customers, keeping pace with rising threats and securing the trust relationships demanded in today's digital world is a must. Trust is not merely a product/service, but also the essential element to engage in online exchange at all, so much so that partnering with the right security provider, one that safeguards not only the ISP/TELCO but also its customers and their data, is crucial for future-proofed business.

With more discerning customers fretting about secure connections and data than ever before, ISPs and TELCOs will need to differentiate themselves via the security solutions they offer, including whether there's an option to add an extra layer like DNS security to the customer's plan. Providing this additional level of service, in partnership with security vendors, not only benefits end users but enhances the provider's reputation.

For their part, cybersecurity vendors have also had to evolve over the last 30 years, from protecting and securing hardware, to valuable data, and increasingly, to securing personally identifiable data. In league with ISPs and TELCOs, it can be accurately said that security vendors now aim to protect users' digital lives. Central to this mission is DNS protection, which offers widespread benefits. DNS protection coupled with router security are straightforward ways to safeguard numerous households, especially where both internet service subscriptions and mobile data are in use.

The use case extends also to high-traffic locations like cafes, restaurants, hotels, airports, and hospitals, where providing public Wi-Fi access is common; in these locations DNS solutions offer

a very safe and user-friendly choice. Consider a hospital with a single network catering to over a thousand daily patients, not counting visitors and staff. This network simultaneously stores critical medical data and likely also supports many other professional and even personal online activities. Here, security challenges can mushroom from the rather open network access required – where anyone, including potential malicious actors, might connect and exploit the network.

Cybercrime is not going anywhere
Cybercrime remains an enduring and ever-evolving challenge in our connected world. To foster a safer online environment, individuals must prioritize their digital safety. However, TELCOs and ISPs are emerging as the entities with the most agency, and possibly the primary responsibility for addressing these risks. By exploring DNS protection in league with security vendors can enable rapid deployment of more robust security measures where needed.

Consumers' growing concern about security and privacy has signaled that TELCOs and ISPs must address these worries proactively. And, given the pervasive nature and substantial economic impact of cybercrime, it's crucial for all stakeholders to take it seriously. Many of these attacks target consumers directly, creating a strong demand for accessible yet powerful security solutions. In today's data-driven landscape, where vast amounts of information are collected and utilized, the need for enhanced protection is gaining momentum. This presents a significant opportunity for TELCOs and ISPs to meet the growing demand for secure digital experiences based on trust.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here