Security Now! #888 - 09-13-22

The EvilProxy Service

This week on Security Now!

This week we look at an unusual and disturbing escalation of a cyberattack. I also note that cryptoheists have become so pervasive that I'm not mentioning them much anymore. The While House conducted a “Listening Session” to dump on today's powerful tech platforms, and a government regulator in The Netherlands quit his position and tells us why. There's another QNAP mess which is bad enough to exceed my already quite high QNAP mess threshold, and D-Link routers need to be sure they are running their very latest firmware. I have another comment about my latest Sci-Fi author discovery and two quick bits of feedback from our listeners. Then we're going to examine EvilProxy, the conceptual cousin to Ransomware as a Service.

Those pesky fuses kept blowing…

Security News

Cyberwarfare: Albania vs Iran

Risky Business News headlined their story this way: “Albania cuts diplomatic ties with Iran in first-ever cyber-related escalation.” I don't have any strong emotional ties to either Albaina or Iran, though it's worth noting that Albania is a member of NATO. Fortunately, at this time, cyberwar mostly amounts to a local inconvenience. But what's so worrisome about this is that it feels as though it's predictive of worse things to come, eventually perhaps involving global scale adversaries. Here's what happened:

The Albanian government announced last Wednesday, the 7th, that it would be cutting all diplomatic relations with Iran in the aftermath of a major cyberattack, marking the first time ever a cyberattack has escalated this severely in the political realm.

In a recorded video statement published on YouTube, (https://youtu.be/j2AJDaFDRro) Albania's Prime Minister Edi Rama said that after concluding an investigation into the incident, they found “indisputable evidence” that Iranian state-sponsored hackers were behind the cyberattack that took place nearly two months prior on July 15, which crippled multiple Albanian government IT systems.

Rama gave Iranian diplomats one day, 24 hours, to close their embassy and exit the country. While the Iranian government denied being involved in the attack, NATO, the White House, and the UK government published statements in support of the Albanian government and supported its attribution of the attack to the Tehran regime. The US called Iran's attack on its NATO ally a “troubling precedent” and promised to “take further action to hold Iran accountable.”

Though Iranian political officials may deny their involvement, the proof lies in the malware used in the July 15 attack, which both Mandiant and Microsoft have linked back to multiple past instances of Iranian cyber-espionage operations and tooling.

Microsoft, which has participated in the Albanian government's response to the incident, said it was able to link the incident to four different Iranian APTs (advanced persistent threat groups), and detailed how these four groups have been working together to breach Albanian government networks at least since last year to establish the proverbial foothold. Then finally in July, the Iranian government decided it was time to act.

Microsoft says the four groups appear to work under the guidance and control of the Iran Ministry of Intelligence and Security (MOIS). The groups are:

- DEV-0842 deployed the ransomware and wiper malware
- DEV-0861 gained initial access and exfiltrated data
- DEV-0166 exfiltrated data
- DEV-0133 probed victim infrastructure

Both Mandiant (which Google purchased in March for $5.4 billion) and Microsoft say the Iranian attack is directly connected to the Albanian government harboring thousands of Iranian dissidents part of an exiled opposition party named the People's Mujahideen Organization of Iran, also known as MEK.

At the request of the US government, MEK was given shelter in Albania in 2016, after the Iranian regime declared the group a terrorist organization and started hunting its members. MEK members were planning to hold an annual summit on July 21. But that summit, “The Free Iran World Summit” was canceled because of terrorist and bomb threats. Microsoft says that the threats and the July 15 cyberattacks were part of a broader effort from the Iranian government to go after the group and its host country.

However, whereas past operations typically involved coordinated social media campaigns, data leaks, vague threats and declarations from Iranian officials, the deployment of a data wiper and ransomware appears to have crossed a line which Albanian and NATO officials are not taking quietly. Though Albanian's prime minister tried to play down the aftermath of the July 15 attack and said that government systems were now restored, the attack crippled government operations and official websites for weeks. In fact, moments after Iranian officials left the embassy, Albanian police raided the building in search of any incriminating evidence that may have survived the typical hard-drive bashing and document-burning practices of fleeing diplomats. Conducting this raid was seen as extreme, but the general sentiment is that NATO partners backed and pushed Albania into this action as a way to signal to other "cyber" aggressive countries that a line is being crossed when entire government IT networks are being wiped just because someone wants to attack a dissident group.

And, if that was the end of it, it would not be good. But it wasn't the end.

As I said, last Wednesday the 7th, Iran's diplomats were given one day to close their embassy and leave the country. Two days later, last Friday the 9th, Albania was hit by another major cyberattack, which has officials once again pointing the finger at Iran. The attack hit Albania's Total Information Management System (TIMS), which is an IT platform belonging to Albania's Ministry of Interior used to keep track of people entering and leaving the country.

According to a series of tweets from Albania's Minister of the Interior, six border crossing points were impacted and experienced border crossing stoppages and delays for at least two days. This included five land crossings including Greece, Kosovo, several in Montenegro and at the Airport near Albania's capital. Ministry officials blamed the attack on "the same hand" that hit Albania's IT network in July, an attribution that was also backed up by the US White House a few hours later.

Perhaps this is an aberration and doesn't reflect the future. I would like to think so. But I'm not hopeful.

Crypto Heist — this or that

I feel that I should note something else that I'm seeing constantly which I just skip over without comment for this podcast: And that's crypto-heists of this or that also-ran cryptocurrency from this or that random exchange no one's ever heard of, or random newbies being crypto-scammed. This week I'll give everyone three perfect typical examples so that everyone has a feeling for what their normally not missing:

First: The New Free DAO (NFD) token lost 99% of its value after a threat actor used a flash loan attack to steal more than $1.25 million worth of crypto from the platform. According to blockchain security firm CertiK, the hacker appears to be the same attacker who also hit DeFi platform Neorder four months ago. (Gripping news, I know.)

Second: The operators of the Gera cryptocurrency suspended operations last week after a hacker gained control over the platform's "smart contract" (which apparently isn't so smart) after developers leaked the private key. According to the Gera team, the attacker minted $1.5 million worth of crypto, which they later transferred to their own Ethereum address. The platform has not yet resumed operations. (Boo hoo.)

And, Third: Romanian law enforcement raided two penthouses in Bucharest and detained three suspects. According to a joint investigation with the UK's National Crime Agency, the suspects would contact victims of cryptocurrency fraud and defraud them again by posing as financial fraud recovery specialists and ask for a substantial fee to recover their initial losses.

Just so everyone knows, there is now a more or less constant flux of these sorts of heists. I see news of them every week but they don't make the cut and I don't think they should.

The White House "Tech Platform Accountability" Listening Session

Last Thursday the US White House conducted one of their "Listening Sessions" — this one on the topic of "Tech Platform Accountability." Though this is not about security, it's arguably one of the hottest and most interesting questions today: In a nation founded on the principle of a right to free and open public speech and a free and open press — neither being under the thumb of the government — what responsibility do our social media platforms have, if any, about the content their users publish and which they subsequently host and our search engines find and index?

I looked through the list and the titles of the 16 attendees who were invited to participate in this "Listening Session" last week. If it were possible for bureaucracy to reach a critical mass where its own gravitational attraction would cause it to collapse in upon itself, putting this group into a single room would be inadvisable. Nevertheless, the listening session occurred and everyone appears to have survived.

I suppose that a session titled "Tech Platform Accountability" would tend toward the negative. But boy, did this group dump on today's social media offerings. The White House started everyone off with a negative tone and the meeting's participants appear to have willingly added fuel. The summary of the event is not long, and I think it's worth sharing. Here's the White House's summary:

> *Although tech platforms can help keep us connected, create a vibrant marketplace of ideas, and open up new opportunities for bringing products and services to market,* [Okay, just so everyone knows, that's the end of the good news part of the summary.] *they can also divide us and wreak serious real-world harms.*
>
> *The rise of tech platforms has introduced new and difficult challenges, from the tragic acts of violence linked to toxic online cultures, to deteriorating mental health and wellbeing, to basic*

> *rights of Americans and communities worldwide suffering from the rise of tech platforms big and small.*
>
> *Today, the White House convened a listening session with experts and practitioners on the harms that tech platforms cause and the need for greater accountability. In the meeting, experts and practitioners identified concerns in six key areas: competition; privacy; youth mental health; misinformation and disinformation; illegal and abusive conduct, including sexual exploitation; and algorithmic discrimination and lack of transparency.*
>
> *One participant explained the effects of anti-competitive conduct by large platforms on small and mid-size businesses and entrepreneurs, including restrictions that large platforms place on how their products operate and potential innovation. Another participant highlighted that large platforms can use their market power to engage in rent-seeking, which can influence consumer prices.*
>
> *Several participants raised concerns about the rampant collection of vast troves of personal data by tech platforms. Some experts tied this to problems of misinformation and disinformation on platforms, explaining that social media platforms maximize "user engagement" for profit by using personal data to display content tailored to keep users' attention—content that is often sensational, extreme, and polarizing. Other participants sounded the alarm about risks for reproductive rights and individual safety associated with companies collecting sensitive personal information, from where their users are physically located to their medical histories and choices. Another participant explained why mere self-help technological protections for privacy are insufficient. And participants highlighted the risks to public safety that can stem from information recommended by platforms that promote radicalization, mobilization, and incitement to violence.*
>
> *Multiple experts explained that technology now plays a central role in access to critical opportunities like job openings, home sales, and credit offers, but that too often companies' algorithms display these opportunities unequally or discriminatorily target some communities with predatory products. The experts also explained that that lack of transparency means that the algorithms cannot be scrutinized by anyone outside the platforms themselves, creating a barrier to meaningful accountability.*
>
> *One expert explained the risks of social media use for the health and wellbeing of young people, explaining that while for some, technology provides benefits of social connection, there are also significant adverse clinical effects of prolonged social media use on many children and teens' mental health, as well as concerns about the amount of data collected from apps used by children, and the need for better guardrails to protect children's privacy and prevent addictive use and exposure to detrimental content. Experts also highlighted the magnitude of illegal and abusive conduct hosted or disseminated by platforms, but for which they are currently shielded from being held liable and lack adequate incentive to reasonably address, such as child sexual exploitation, cyberstalking, and the non-consensual distribution of intimate images of adults.*
>
> *The White House officials closed the meeting by thanking the experts and practitioners for sharing their concerns. They explained that the Administration will continue to work to address the harms caused by a lack of sufficient accountability for technology platforms. They further stated that they will continue working with Congress and stakeholders to make bipartisan progress on these issues, and that President Biden has long called for fundamental legislative reforms to address these issues.*

It seems clear that sooner or later we're going to be subjected to legislation as our various governments' attempt to somehow micro-manage this incredibly slippery terrain which, at least in the United States, enjoys Constitutionally-protected freedoms. So I want to finish by sharing the six bullet-point targets which were cited as "core principles for reform":

1. ***Promote competition in the technology sector.*** *The American information technology sector has long been an engine of innovation and growth, and the U.S. has led the world in the development of the Internet economy. Today, however, a small number of dominant Internet platforms use their power to exclude market entrants, to engage in rent-seeking, and to gather intimate personal information that they can use for their own advantage. We need clear rules of the road to ensure small and mid-size businesses and entrepreneurs can compete on a level playing field, which will promote innovation for American consumers and ensure continued U.S. leadership in global technology. We are encouraged to see bipartisan interest in Congress in passing legislation to address the power of tech platforms through antitrust legislation.*

2. ***Provide robust federal protections for Americans' privacy.*** *There should be clear limits on the ability to collect, use, transfer, and maintain our personal data, including limits on targeted advertising. These limits should put the burden on platforms to minimize how much information they collect, rather than burdening Americans with reading fine print. We especially need strong protections for particularly sensitive data such as geolocation and health information, including information related to reproductive health. We are encouraged to see bipartisan interest in Congress in passing legislation to protect privacy.*

3. ***Protect our kids by putting in place even stronger privacy and online protections for them, including prioritizing safety by design standards and practices for online platforms, products, and services.*** *Children, adolescents, and teens are especially vulnerable to harm. Platforms and other interactive digital service providers should be required to prioritize the safety and wellbeing of young people above profit and revenue in their product design, including by restricting excessive data collection and targeted advertising to young people.*

4. ***Remove special legal protections for large tech platforms.*** *Tech platforms currently have special legal protections under Section 230 of the Communications Decency Act that broadly shield them from liability even when they host or disseminate illegal, violent conduct or materials. The President has long called for fundamental reforms to Section 230.*

5. ***Increase transparency about platform's algorithms and content moderation decisions.*** *Despite their central role in American life, tech platforms are notoriously opaque. Their decisions about what content to display to a given user and when and how to remove content from their sites affect Americans' lives and American society in profound ways. However, platforms are failing to provide sufficient transparency to allow the public and researchers to understand how and why such decisions are made, their potential effects on users, and the very real dangers these decisions may pose.*

6. ***Stop discriminatory algorithmic decision-making.*** *We need strong protections to ensure algorithms do not discriminate against protected groups, such as by failing to share key*

> *opportunities equally, by discriminatorily exposing vulnerable communities to risky products, or through persistent surveillance.*

We're all aware of this battle which has been simmering and is growing hotter. And many people have chosen a position. In my opinion, as a technologist, it will be a significant challenge to do the right thing. But we can't even start until we decide what the right thing is. Technology often presents mankind with difficult problems and decisions. In the case of the Internet, we have a single global network carrying services which straddles nations whose governments grant their citizenry widely differing rights and which restrict the behavior of their enterprises in widely differing ways. How does a single Facebook, Twitter, Instagram or Google service simultaneously satisfy the differing requirements of all? Some very interesting problems lay ahead.

And before we leave the interesting subject of governments, here's another little tidbit from The Netherlands:

Changes to the Dutch Intelligence Law:
Bert Hubert, a member of TIB, the Dutch government board that checks the legality and approves communications interception warrants for the Dutch intelligence and security services, resigned last week. The automatic English translation of Bert's blog posting explaining his decision was so atrocious that he wrote an English version himself. And I'm so glad he did, because if I were serving in a government that I believed in, I'd hire this guy in a second. Here's what Bert wrote:

> *If either of the civil or the military intelligence and security services of The Netherlands want to use their lawful intercept, SIGINT or hacking (& some other) legal powers, they have to first convince their own jurists, then their ministry and finally the TIB. The TIB then studies if the warrant is legal, and that decision is binding.*
>
> *When I joined the regulatory commission, I was very happy to find that the Dutch intelligence and security services were doing precisely the kinds of things you'd expect such services to do. I also found that our regulatory mechanisms worked as intended - if anything was found to be amiss, the services would actually stop doing that. If the ex-ante regulator* [meaning up front in advance] *(ie, my board) ruled a permission to do something was unlawful, it would indeed not happen. I think it is important to affirm this in public.*
>
> *Over the past two years however there have been several attempts to change or amend the Dutch intelligence law. The most recent attempt has now cleared several legislative hurdles and looks set to be passed by parliament.*
>
> *Under this new law, my specific role (technical risk analysis) would mostly be eliminated. In addition, the Dutch SIGINT (bulk interception) powers would be stripped of a lot of regulatory requirements. Furthermore, there are new powers, like using algorithmic analysis on bulk intercepted data, without a requirement to get external approval. Finally, significant parts of the oversight would move from up front ('ex ante') to ongoing or afterwards ('ex post').*
>
> *Doing upfront authorization of powers is relatively efficient, and is also pleasingly self regulating. If an agency overloads or confuses its ex ante regulator, they simply won't get permission to do things. This provides a strong incentive for clear and concise requests to the regulator.*

> *A regulator that has to investigate ongoing affairs however is in a different position. It can easily become overloaded, especially if it is unable to recruit sufficient (technical) experts. In the current labor market, it is unlikely that a regulator will be able to swiftly recruit sufficient numbers of highly skilled computer experts able to do ongoing investigations of sophisticated hacking campaigns and bulk interception projects. An overloaded regulator does not provide good coverage. It is also vulnerable to starve the beast tactics.*
>
> *Once it became clear the intended law would likely pass parliament, I knew I would have to resign anyhow, since I don’t agree with the new expanded powers and the changes in oversight.*
>
> *As a member of the regulatory board, I could not share my worries about the new law. The regulatory board itself is staffed with excellent people, but by design, the board only operates within the existing law. It is not responsible for formulating or even criticizing any new laws.*
>
> *Instead of waiting out the likely passing of the new law, I’ve decided to leave now. This enables me to speak my mind on what is wrong with the new law. It may not help, but at least it is better than watching* ***democratic backtracking*** *in silence.*
>
> *It has been a great honor to have been part of the regulatory powers board. Its staff and members are an impressive bunch, and I wish them the best of luck with their ongoing and important work.*
>
> *On a final note, if anyone is looking for a government regulator with a proven track record of resigning when things go wrong, know that I’m available.*

It’s also worth noting, though Bert didn’t mention it in his blog posting, Bert’s TIB flagged several cases of abuse last year that targeted journalists and several cases of broad warrants that intercept bulk traffic over entire global internet cables.

Bert’s term for what he sees happening is “democratic backtracking.” I thought this was worth sharing since it shows the way democracy will decay if it’s not fully understood and continually reinforced. It is not an inherently stable system since it is subject to creeping manipulation. Some group of right-minded people originally established the operation of the Dutch regulatory commission to work the way it does today for a reason; for at least some of the reasons Bert has explained. But maybe those who did this are now out of power, and those being regulated have been chafing at the limitations the current system deliberately imposes upon them. Yes, it’s inconvenient and annoying. It’s meant to be. Surveillance of a free and democratic people should not be the default; it should be the exception. And it does seem that initiating the surveillance first and asking for permission either concurrently or afterward is far more likely to lead to abuse. Again, the question is, what principles do we want to support?

Another QNAP mess:

Another near-constant event that I choose to only cover periodically is horrendous problems occurring in QNAP NAS software. Since it's entirely possible to run a non-QNAP OS on their QNAP hardware, I dearly hope that anyone listening to this podcast will have switched out QNAPs constantly disappointing firmware for any of the Linux or Unix alternatives that are known to run. And if you do need to remain with QNAP, please by all means, protect it from the public Internet. We've talked about many ways to do that previously. Even QNAP themselves has told their own users not to expose their devices to the Internet.

So... “Deadbolt” is both a ransomware and a ransomware group that has been plaguing QNAP users and their devices all year. Since January, thousands of QNAP customers have reported being attacked by the DeadBolt ransomware group. The group demands a ransom of 0.03 Bitcoin — currently around $1,100 — for the decryption key.

After the initial attacks affecting about 3,600 devices last January, the group continued to resurface with campaigns in March, May, and June this year. Reddit and other message boards have been flooded with customers lamenting the loss of files that included family photo albums, wedding videos and more. Dozens of users took to Reddit to complain that they were among those attacked in the latest campaign.

In a note to QNAP, the hackers demanded 5 Bitcoin ($93,900) to reveal details about the alleged zero-day vulnerabilities they initially used to attack its users and another 50 Bitcoin ($939,000) to release a master decryption key that would unlock all of the victims’ files.

QNAP would not say whether it has considered paying the ransom for the universal decryption key when asked by The Record. But we can be pretty sure not when a spokesperson said the company’s research has shown that the Deadbolt group is attacking “legacy versions with known vulnerabilities which have security updates available.” In other words, it's the user's fault, so they should pay if they want their data back.

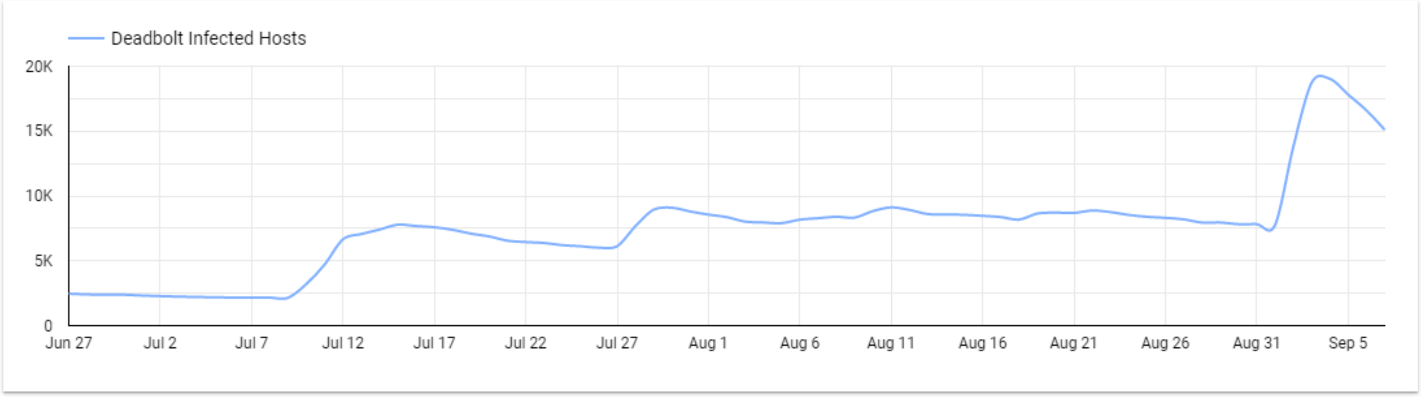
Some users have disputed QNAP’s insistence that only devices that have not been updated are being attacked. And if ransom is paid, the key provided by Deadbolt may not work. So, the security company EmsiSoft released its own version of a DeadBolt decryptor after several victims reported having issues with the one they received in exchange for paying a ransom. However, it's not any sort of universal decryptor. It only works with a decryption key supplied by the operators of the DeadBolt ransomware through a ransom payment. EmsiSoft's Fabian Wosar Tweeted: *“QNAP users who got hit by DeadBolt and paid the ransom are now struggling to decrypt their data because a forced firmware update issued by @QNAP_nas removed the payload that is required for decryption. If you are affected, please use our tool instead.”*

What a mess.

Earlier this year, the security company Censys who runs that IoT search engine, reported that of the total 130,000 QNAP NAS devices sold, 4,988 services *“exhibited the telltale signs of this specific piece of ransomware.”* Censys also managed to track the Bitcoin wallet transactions associated with an infection and found that of the previous batch of victims, 132 paid ransoms totaling about $188,000. The company also created a dashboard to track the number of victims around the world. The majority of the most recent infections are taking place in the U.S., Germany and the United Kingdom.

And it's not over...

This mess finally rose above my already high QNAP ongoing-exploit-of-the-moment threshold because Censys observed that the number of QNAP NAS devices infected by, yes, the Deadbolt ransomware, spiked from 2,144 on July 9 to 19,029 on September 4, Sunday before last.



The spike arose when the ever industrious Deadbolt gang exploited a 0-day vulnerability in the Photo Station app installed on most QNAP NAS systems. So, they're still finding new ways in.

If you have a QNAP NAS with QNAP software, get it off the Internet.

Operator (or Admin) Error

Before we leave the Censys Internet scanning company, it's worth noting that their recently published "2022 State of the Internet Report" observed that misconfigurations accounted for 60% of the issues they observed across all Internet-exposed services. Software that was actually vulnerable only accounted for 12% of all observed problems. It's unclear whether placing a QNAP NAS onto the Internet would inherently be considered a misconfiguration of those devices, but it seems pretty clear that it should be.

D-Link's being taken over by MooBot

Palo Alto Networks' Unit 42 has identified a three year old Mirai Botnet variant known as MooBot. It is rapidly finding and co-opting any remaining vulnerable D-Link routers into another army of denial-of-service bots by taking advantage of multiple old and new, but all long since patched, exploits.

Last Tuesday, Unit 42 wrote: *"If the devices are compromised, they will be fully controlled by attackers, who could utilize those devices to conduct further attacks such as distributed denial-of-service (DDoS)."*

MooBot, which was first identified and disclosed by Qihoo 360's Netlab team in September 2019, has previously targeted LILIN digital video recorders and those Hikvision video surveillance products we were talking about a couple of weeks ago. In the latest wave of attacks discovered by Unit 42 early last month, as many as four different highly critical flaws in D-Link devices are being used in the deployment of MooBot samples. The four flaws are:

- CVE-**2015**-2051 (CVSS score: **10.0**) - D-Link HNAP SOAPAction Header Command Execution Vulnerability
- CVE-**2018**-6530 (CVSS score: **9.8**) - D-Link SOAP Interface Remote Code Execution Vulnerability
- CVE-**2022**-26258 (CVSS score: **9.8**) - D-Link Remote Command Execution Vulnerability, and
- CVE-**2022**-28958 (CVSS score: **9.8**) - D-Link Remote Command Execution Vulnerability

Successful exploitation of any **ONE** of those four flaws, which all have very low attack complexities, is used to remotely launch a WGET command which retrieves the MooBot payload from a remote host. MooBot then parses instructions from a command-and-control (C2) server to launch DDoS attacks in ways we are all too familiar with.

Although the oldest vulnerability is from 2015 and the next oldest is from 2018, the other two were found and fixed this year. So anyone who knows anyone who uses a D-Link router should be certain that they have updated recently.

Sci-Fi Discovery

"The Silver Ships" - http://scottjucha.com/silverships.html
Last week, I introduced our listeners to my latest science fiction reading discovery, Scott Jucha's "The Silver Ships" thanks to one of our listeners. I have been having **so** much fun ever since. I'm now halfway through the 4th book and I can assert that this is the most engaging and satisfying series of novels I've read in a long long time. And just wait until you meet the Swei Swee. For those of you who prefer to have books read to them, I'm so glad that Leo said that the reader of this series is someone he knows and enjoys listening to... because I wouldn't want anything to spoil the experience of Audible's listeners.

My initial mild concern after only the first book, that Scott Jucha's character development might be overly focused upon his story's central character, Alex Racine, has dissolved completely. We now have a broad cast of wonderful characters. This guy writes **so** wonderfully.

I was trying to put into context for myself how good this book series is. I know that there have been times in the past when I have been this thrilled over a science fiction storyline. The Honor Harrington novels, Michael McCullum's Gibraltar Stars trilogy. And I'm sure that some of Peter Hamilton's stories did this, though they are always a lot to wade through. And there must be others, since it's a familiar feeling for me to be **so satisfied** when reading the inventions of a skilled storyteller who really knows how to weave a yarn and who has come up with a bunch of great new sci-fi technologies, and people, both human and non. Another thing I've noticed is that, like the best serialized stories, a **lot** happens in every installment. So far there has been no sense of Scott stringing us along. Even when the action slows down for a while, there turns out to be real purpose in the way we were spending that time.

The best books are those that cause you to immediately wish for amnesia so that the story can be experienced again, new. This series is the equal of any I've read. And prepare yourself for a huge surprise at the start of book #3.

Closing The Loop

x4jw / @x4jw

> *Hi Steve. Thanks for the recommendation of The Silver Ships series of books. Went to purchase Book 1 on my Audible account and was surprised/delighted to see that Books 2,3,4,5,7,8,9 are all included for "free" as part of the Audible Plus membership and I just had to click ADD TO LIBRARY to grab those. I can understand why Book 1 is not free... Not sure why Book 6 isn't. Books 10-20 are also purchase-to-own titles on Audible. Anyway... just thought "readers" using Audible might like to know they can get 35% of the series for free as part of the Plus subscription service. Thanks for all that you do. Kind Regards. Tim from Melbourne, Aust.*

RobinR / @robinr1981

> *Hi Steve, I'm a big fan of yours and Security Now. I highly respect your knowledge and your way of explaining things. I was wondering if you could share what you feel allows you to be so productive. I don't mean to pry into your personal life, but more curious how you manage your time to do so many things. Just off the top of my head: 1) Deep preparation for Security Now 2) Troubleshooting/debugging Spinrite to make it perfect 3) Keeping up with super long sci fi novels 4) Recommending sci fi shows 5) Managing your company, etc I know I haven't even touched the surface, but if you are inclined to share your productivity tips or how you manage your time, I would love to hear it. I know that some of it is individual to the person, but I'm sure there are some common things that apply to productive people like yourself.*

The key to my appearing to be so productive is that I've been fortunate to be able to craft a life where I really enjoy every hour that I spend. I truly love technology and computing and I've been able to make a life out of that which I love. I could burn a lot of time in front of a Television screen if I wanted to. But I don't, because there is so much else that I find more interesting.

And I guess, also, it's that I really **like** to work. I enjoy creating things; whatever they may be.

I've sometimes encountered someone online offering something and saying that maybe it could be better but they were "too lazy" to put more effort into it. Too lazy!! Can you imagine hearing me say that? I have never felt the tiniest shred of that in my entire life. It must be that the person saying that doesn't care. But how can you not care about something you're choosing to do? I guess it's mostly that the mystery and puzzle of life really interests me and that I'm still really excited — even after 67 years — to still be here working to solve the puzzle. :)

The EvilProxy Service

https://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web

Last Monday, the security research group called Resecurity published their findings about a recently appearing (last May) new, fully functional, turnkey, Phishing-as-a-Service system known as EvilProxy. Key among the many powerful features of this new underground service debuting on the Dark Web is its effortless ability to intercept SMS, Oauth and TOTP multi-factor authentication flows. As a result, the "Login with some other website" like Google or Facebook, or enter the SMS code we just sent to your phone, or enter the 6-digit code displayed on your authenticator... are all effortlessly bypassed and rendered ineffective.

This is all accomplished by streaming the actual target website, where the naïve user believes they are logging in, through a transparent reverse proxy — which I'll explain further in a minute. They are not actually where they think they are. And unless they are scrupulously attentive to the URL being displayed in their browser's URL bar, they will be unwittingly providing their full authentication credentials, including **any** form of multi-factor authentication, to a malicious third-party who will intercept their successful login session token to obtain a full secondary login to their account — with all the rights that arise from that.

This sort of proxying is one of the inherent Achilles heel's of the way the web works. One summer, when I was deep into the work on SQRL, I brought my work to a halt in order to completely wrap my head around this spoofing problem, because it's a tough one. I felt as though I still didn't have an absolutely crystal clear understanding of exactly where the problem arose, and I needed SQRL to solve it. I figured it out and the result was something we call CPS, for Client Provided Session; and it does, indeed, once and for all, completely solve this problem. Since I'm at work on SpinRite v6.1 I haven't taken the time to determine whether the FIDO2 and WebAuthn folks also solved this problem. And it doesn't matter whether it does or not, since the Passkeys system is what we'll eventually be getting. But for what it's worth, it is possible to completely solve it and that's another of the, perhaps unique things, that SQRL does.

Anyway, remember the wonderful observation which we credit to Bruce Schneier: "Attacks never weaker, they only ever get stronger." We're about to see an example of Bruce's observation, on steroids. The thing that is so chilling about this new EvilProxy service is exactly that: It's a service. The horrifying Log4j JAVA vulnerability is certainly a problem. But as we've previously described, it turned out not to be the end of the world for one reason: It was not a slam-dunk, drop and go, easy to use vulnerability. Every specific instance of its use needed to be deliberately engineered for the specific target where that potential vulnerability might be exploited. And the industry learned an important lesson from that: It matter far less whether something is possible than whether it's easy to use.

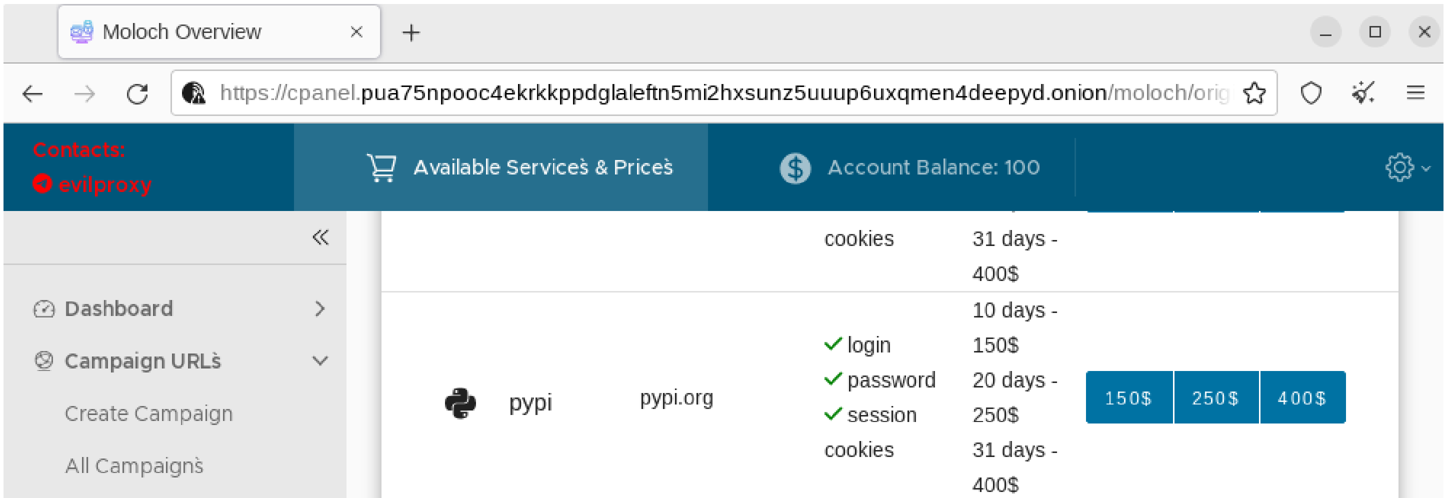
Which brings me to why this new EvilProxy Phishing-as-a-Service facility is so horrifying: The service providers have created an astonishingly powerful, simple to use, point and click web interface for their service. Through this interface, powerful phishing campaigns can be created by filling out some fields, selecting the required features, and pressing a create campaign button. If the Log4J vulnerability never exploded because it was difficult to use, this EvilProxy service promises to be an instant hit because it could hardly be any easier to use. So that everyone can see this for themselves, this week's GRC shortcut of the week https://grc.sc/888 (https://vimeo.com/746020364) ... will bounce its user's browser over to a 4-minute Vimeo video (number 746 020 364) which the EvilProxy service provider uses to market and demo the ease-of-use of their tool.

Okay. So now let's back up a bit for a bit broader overview of Resecurity's discovery from coverage of this. The title of their report was "EvilProxy Phishing-As-A-Service With MFA Bypass Emerged In Dark Web" and they wrote:

> *Following the recent Twilio hack leading to the leakage of 2FA (OTP) codes, cybercriminals continue to upgrade their attack arsenal to orchestrate advanced phishing campaigns targeting users worldwide. Resecurity has recently identified a new Phishing-as-a-Service (PhaaS) called EvilProxy advertised in the Dark Web. On some sources the alternative name is Moloch, which has some connection to a phishing-kit developed by several notable underground actors who targeted the financial institutions and e-commerce sector before.*
>
> *While the incident with Twilio is solely related to the supply chain, cybersecurity risks obviously lead to attacks against downstream targets, the productized underground service like EvilProxy enables threat actors to attack users with enabled MFA on the largest scale without the need to hack upstream services.*
>
> *EvilProxy actors are using Reverse Proxy and Cookie Injection methods to bypass 2FA authentication – proxyfying victim's session. Previously such methods have been seen in targeted campaigns of APT and cyberespionage groups, however now these methods have been successfully productized in EvilProxy which highlights the significance of growth in attacks against online-services and MFA authorization mechanisms.*
>
> *Based on the ongoing investigation surrounding the result of attacks against multiple employees from Fortune 500 companies, Resecurity was able to obtain substantial knowledge about EvilProxy including its structure, modules, functions, and the network infrastructure used to conduct malicious activity. Early occurrences of EvilProxy have been initially identified in connection to attacks against Google and MSFT customers who have MFA enabled on their accounts – either with SMS or Application Token.*
>
> *The first mention of EvilProxy was detected early May 2022, this is when the actors running it released a demonstration video detailing how it could be used to deliver advanced phishing links with the intention to compromise consumer accounts belonging to major brands such as Apple, Facebook, GoDaddy, GitHub, Google, Dropbox, Instagram, Microsoft, Twitter, Yahoo, Yandex and others.*
>
> *Notably, EvilProxy also supports phishing attacks against Python Package Index (PyPi):*

And in their report they embed a screenshot from the EvilProxy control panel showing the entry and options for proxying PyPI login and authentication. It shows that login, password and session cookies are supported, and the user can choose to have the service running for 10 days for $150, 20 days for $250, or 31 days for $400. So, your typical quantity discount schedule. Up at the top of the page we see a .onion URL, so this is being hosted by a hidden Tor Project Onion Service. And below is the control panel page selector showing a shopping cart icon labeled

“Available Services & Prices” next to a circled dollar sign icon labeled “Account Balance”:



https://cpanel.pua75npooc4ekrkkppdglaleftn5mi2hxsunz5uuup6uxqmen4deepyd.onion/moloch/orig

		cookies	31 days - 400$	
pypi	pypi.org	✓ login ✓ password ✓ session cookies	10 days - 150$ 20 days - 250$ 31 days - 400$	150$ 250$ 400$

Conveniently, on the left, is an expandable drop-down labeled “Campaign URLs” and underneath that is “Create Campaign.” The Reservice guys addressed the point of targeting software repositories. The said:

> *The official software repository for the Python language (Python Package Index (PyPI)) seid last week that project contributors were subject to a phishing attack that attempted to trick them into divulging their account login credentials. The attack leveraged JuiceStealer (as the final payload after the initial compromise) and according to Resecurity's HUNTER team findings - related to EvilProxy actors who added this function not long before the attack was conducted.*
>
> *Besides PyPi, the functionality of EvilProxy also supports GitHub and npmjs (the JavaScript Package Manager widely used by over 11 million developers worldwide) enabling supply chain attacks via advanced phishing campaigns. It's highly likely the actors aim to target software developers and IT engineers to gain access to their repositories with the end goal to hack "downstream" targets. These tactics allow cybercriminals to capitalize on the end users’ insecurity who assume they're downloading software packages from secure resources and don't expect it to be compromised.*

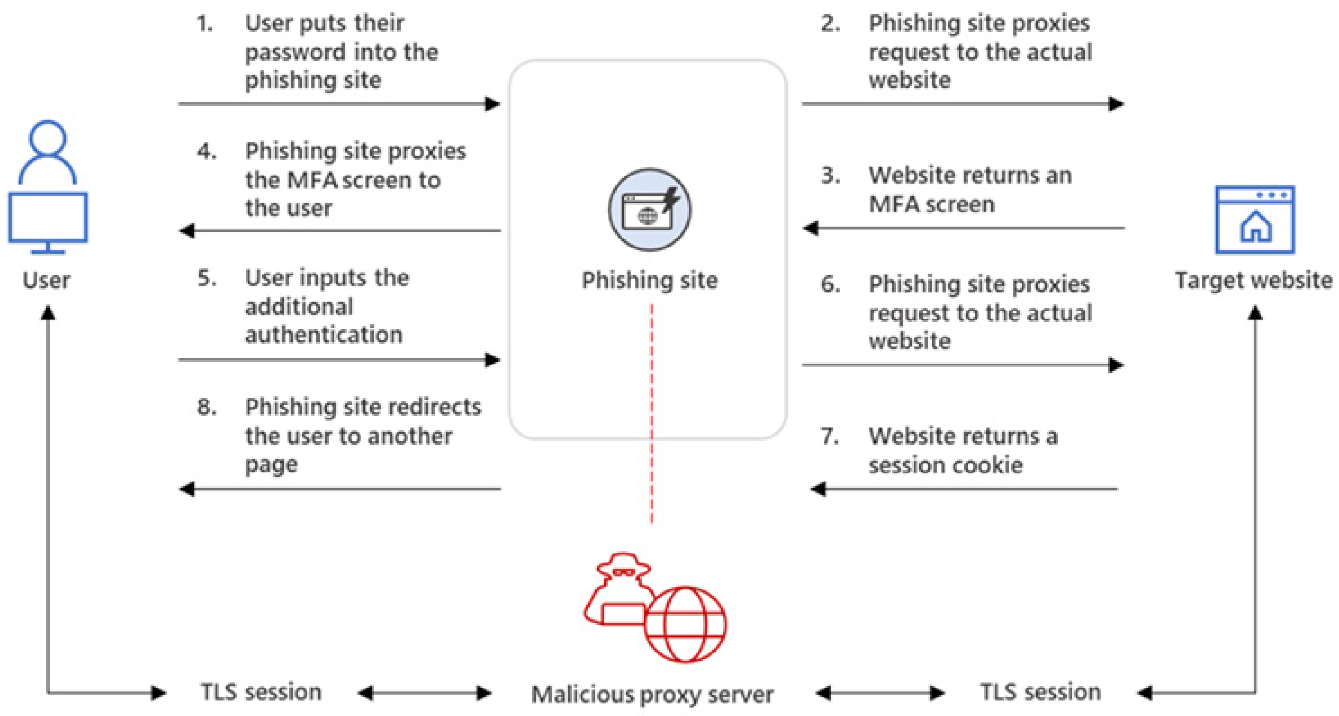
So, how does all of this work?

As I mentioned before, the Internet and the World Wide Web specifically, have an inherent problem which is created by the Web’s brilliantly flexible and powerful underlying technologies.

The URL was originally intended to be fully human readable. Even human typeable. But as we have all watched the evolution of web-hosted services through the past few decades, we’ve seen the readability — and certainly the typeability — of URLs virtually disappear. As I’m typing this text into Google Docs, I look up and see a URL that appears to be mostly random character gobbledygook. And, significantly, I opened and have been editing this document at this point for the past three hours, yet **that** was the first time my eyes fell upon this page’s URL. Why did I have any reason to believe I was in the right place? I was sure I was because the page looked the way I expected it to look. I never had any doubt. So I never sought or received any further confirmation beyond the composition of the page I’m visiting.

I'm one of the hundreds of thousands of people listening to this podcast. I'm one of us. How do we imagine that a **normal** Internet user regards all of the utterly indecipherable things that their web browser does? And we've added all of this script-driven automation to the user's experience, too. When a user clicks on a link in a search engine, on a social media site, or in an eMail, they may have noticed their URL bar flickering rapidly as their browser dances among all of today's various 3rd-party link tracking services. Everyone wants to get in there for a piece of the action. So we've fully eliminated any sense from even an unusually savvy user that they should worry about the details of what's going on there. That's just the way things are today.

EvilProxy leverages the "Reverse Proxy" principle which is made possible by all of this inherent flexibility we've built into the Web. Conceptually, the way it works is simple: the bad guys lead their intended victim to a phishing page. That page uses what's known as a reverse proxy to fetch and display from the legitimate page all of the legitimate content the user expects to see, including login pages - and it sniffs their traffic as it passes through the proxy. It's a classic man-in-the-middle. This "in the middle" position allows the middleman to harvest the valid web browser session cookies which are eventually passed back to the victim user, thus using the victim as an authentication mule to provide the usernames, passwords and even any 2FA tokens.


1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
4. Phishing site proxies the MFA screen to the user
3. Website returns an MFA screen
User
Phishing site
Target website
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
8. Phishing site redirects the user to another page
7. Website returns a session cookie
TLS session
Malicious proxy server
TLS session

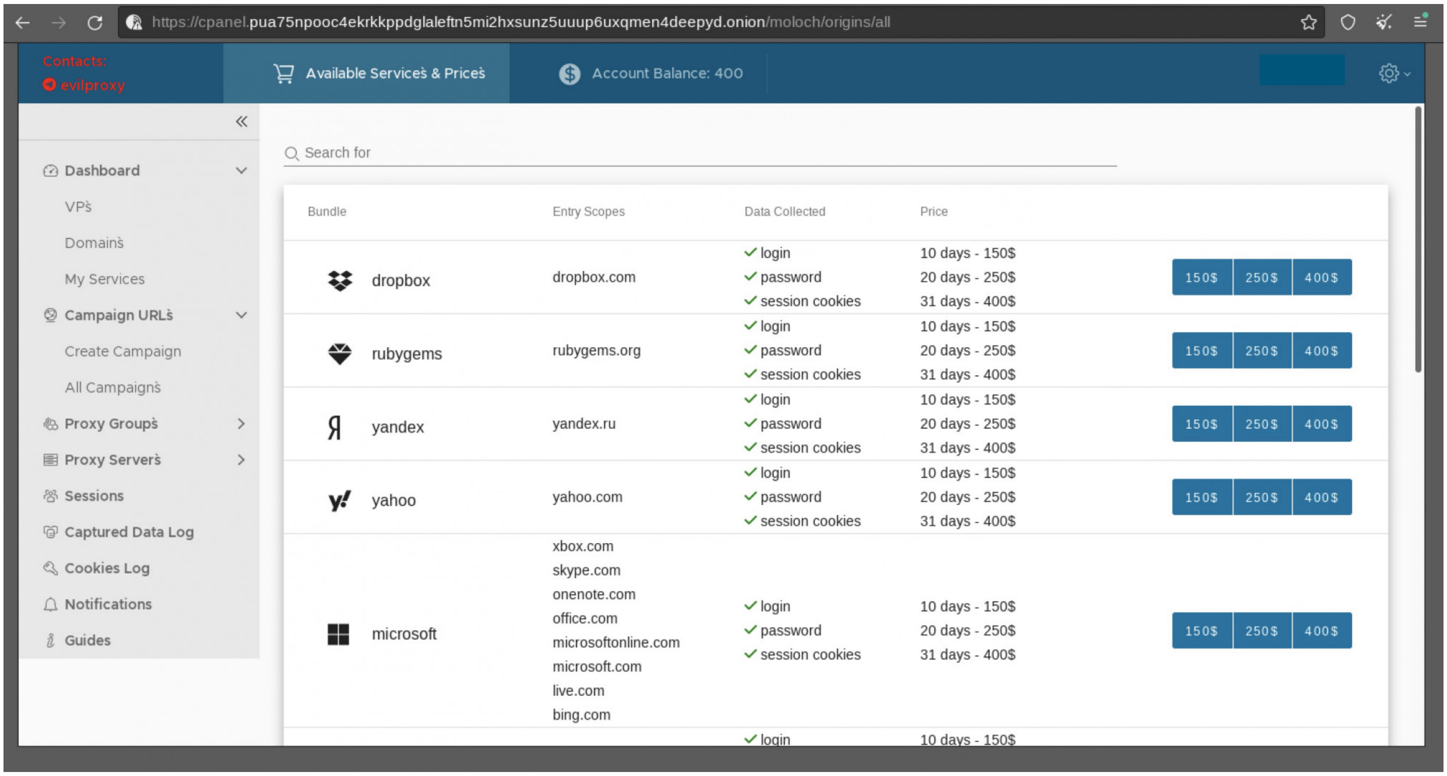
Remember, also, that while the man-in-the-middle is able to intercept and forward one-time tokens for their one-time use, and intercept and obtain the resulting session authentication cookies, because the reverse proxy terminates TLS encryption in each direction, it sees everything in the clear. This means that anyone NOT using some form of additional one-time multifactor authentication will have their username and password stolen in the clear for future use.

The Resecurity guys obtained videos released by the EvilProxy service providers demonstrating the use of their point-and-click setup to steal the victim's session and successfully authenticate through Microsoft 2FA and Google e-mail services to gain access to the target account. The more you see, the more chilling it all is. I've included the link to Resecurity's full report which embeds additional Vimeo videos for anyone who wants to become even more frightened.

https://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web

As I noted above, EvilProxy's services are offered on a pre-paid account balance basis. When the end user cybercriminal chooses a service of interest to target — Facebook, Linkedin, whatever — the activation will be for a specific period of time: 10, 20 or 31 days as described in the plan's itemized description. One of the key actors, using the moniker "John_Malkovich" acts as gatekeeper administrator to vet all new customers. The service is represented on all major underground communities including XSS, Exploit and Breached.

Payments for EvilProxy are arranged manually via an operator on Telegram. Once the funds for the subscription are received, they're deposited into the account in the customer portal hosted in TOR. Use of the service is available for $400 per month in the Dark Web hosted in TOR network.



Bundle	Entry Scopes	Data Collected	Price	
dropbox	dropbox.com	✓ login ✓ password ✓ session cookies	10 days - 150$ 20 days - 250$ 31 days - 400$	150$ 250$ 400$
rubygems	rubygems.org	✓ login ✓ password ✓ session cookies	10 days - 150$ 20 days - 250$ 31 days - 400$	150$ 250$ 400$
yandex	yandex.ru	✓ login ✓ password ✓ session cookies	10 days - 150$ 20 days - 250$ 31 days - 400$	150$ 250$ 400$
yahoo	yahoo.com	✓ login ✓ password ✓ session cookies	10 days - 150$ 20 days - 250$ 31 days - 400$	150$ 250$ 400$
microsoft	xbox.com skype.com onenote.com office.com microsoftonline.com microsoft.com live.com bing.com	✓ login ✓ password ✓ session cookies	10 days - 150$ 20 days - 250$ 31 days - 400$	150$ 250$ 400$
		✓ login	10 days - 150$	

The EvilProxy portal contains tutorials and interactive videos explaining the use of the service and configuration tips. The bad guys did a state-of-the-art job in terms of the service usability, and configurability of new campaigns, traffic flows, and data collection.

After activation, the operator will be asked to provide SSH credentials to further deploy a Docker container and a set of scripts. This approach was likely borrowed from a previous Phishing as a Service called "Frappo" which the Resecurity guys identified earlier this year.

So, in conclusion, what does this all mean?

While access to the EvilProxy service requires individual customer/client vetting, cybercriminals now have a cost-effective and scalable point-and-click solution which provides them with all of the backend machinery required to enable them to run advanced phishing attack campaigns which all of our experience shows will successfully compromise consumers of popular online services — even, and specifically, in the presence of state-of-the-art multi-factor authentication.

The appearance of such a service on the Dark Web **will** undoubtedly lead to a significant increase in account takeover business eMail compromise (ATO/BEC) activity and cyberattacks targeting the identity of end users, where MFA may now be easily bypassed with the help of tools like EvilProxy.

EvilProxy has no corner on the market. All they really did was to fully automate an already existing aspect of advanced cybercrime. They clearly got the idea from the preceding Ransomware as a Service (RaaS) control panels which act just the same. And as we know, those have been **way** too successful for exactly the same reason that EvilProxy promises to be.

And we know what will happen next. Other cretins will see it and decide to compete with it. Once multiple such services exist, competition will drive continued evolution in the features and will also drive down the cost to use them.

We built a very powerful and capable World Wide Web whose features are increasingly being used against us. The creation of reverse proxy exploitation, followed by an easy-to-use turnkey service was probably inevitable, but it’s certainly not good news.