THE UNDERGROUND ECONOMY

The Dark Web and the Rise in Sophisticated Attacks

Trustwave®

THE UNDERGROUND ECONOMY

The Dark Web and the Rise in Sophisticated Attacks

Introduction

THRIVING ON FEAR AND UNCERTAINTY

In light of heightened concerns surrounding public health, political unrest, economic instability and changing workforce dynamics, it's no surprise that the year 2020 and its aftermath sparked a variety of new and often innovative exploits in the world of cybercrime. What is most concerning? How is criminal activity evolving? And what is being done in response? In this guide, we'll expose the latest drivers of the underground economy and what these new threats might look like in your environment.

GOING UNDERGROUND: THE LATEST TRENDS

In difficult times, people become more resourceful out of necessity, and hackers, in particular, have capitalized on this skill in the past year. These examples of recent activity illustrate just how adaptive bad actors can be when opportunities present themselves.

BEYOND HEALTH RISKS: COVID CYBERCRIME

COVID-19 has demonstrated once again that forces driving economic and social change above ground affect underground activity. What's interesting is how varied the responses to the pandemic have been on the Dark Web.

We saw an unexpectedly human aspect from some forum members who expressed fears and shared information while simultaneously witnessing an uptick in phishing scams, malware, and the exploitation of essential resource shortages, such as selling N95 masks and toilet paper at outrageous markups. A code of conduct has held the Dark Web together since its inception. Like the world above, though, it has also experienced increasing amounts of division amongst its members.

Despite occasional moral debate exposing an ironically humane element of the Dark Web, the proliferation of fake vaccines for sale, bogus cures, and even business email compromise scams (also known as CEO fraud) during the pandemic shows how members of this community ultimately take advantage of heightened emotions and their knowledge of human behavior to bait unsuspecting victims.

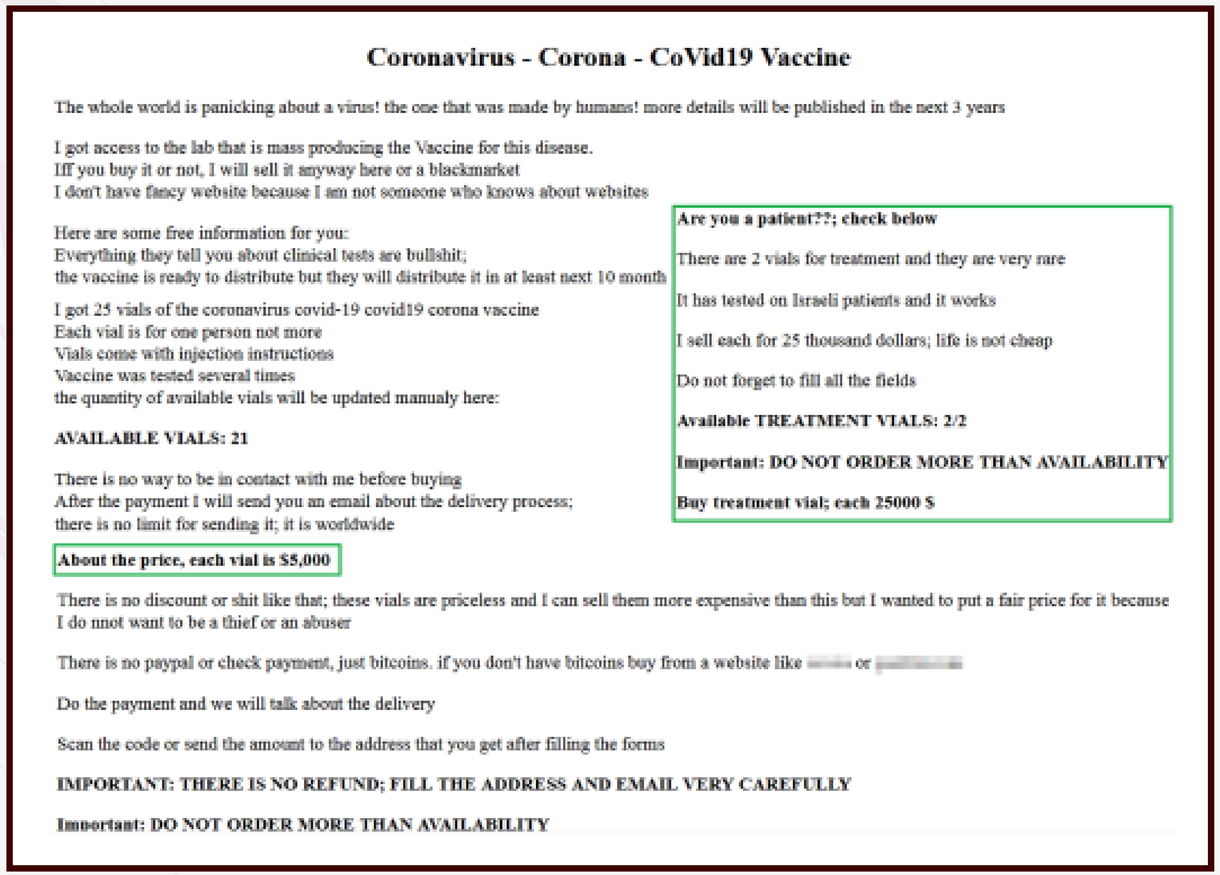
Please Don't Use Your iPhone to Self-Diagnose COVID-19

POSTED BY: DARKNET-DEEP WEB MARCH 24, 2020

The coronavirus is scary for all of us. I've seen one too many stories this weekend about seemingly healthy, young people being hit with COVID-19 and dropping dead within a week's time. I was even tempted to Google symptoms when I had a slight cough and a possibly stuffy nose, because health anxiety is *real*.

With more than 80,000 newly registered domains that contain words such as corona, COVID, Wuhan, and quarantine, created between February and May of 2020 alone, it's easy to see how threats disguised as legitimate information and accelerated by the latest automated techniques gained momentum. Even credible sender and HTML display names, such as CDC.org and the World Health Organization (WHO), can mask malicious PDF downloads and links. Phishing scammers have feasted on these new features, increasing instances of stolen credentials and ransomware threats.

Compounded by what was essentially an overnight transition to a remote workforce, businesses also experienced an elevation in security concerns, including network access and conference software vulnerabilities that bad actors took advantage of quickly.



Coronavirus - Corona - CoVid19 Vaccine

The whole world is panicking about a virus! the one that was made by humans! more details will be published in the next 3 years

I got access to the lab that is mass producing the Vaccine for this disease.
Iff you buy it or not, I will sell it anyway here or a blackmarket
I don't have fancy website because I am not someone who knows about websites

Here are some free information for you:
Everything they tell you about clinical tests are bullshit;
the vaccine is ready to distribute but they will distribute it in at least next 10 month

I got 25 vials of the coronavirus covid-19 covid19 corona vaccine
Each vial is for one person not more
Vials come with injection instructions
Vaccine was tested several times
the quantity of available vials will be updated manualy here:

AVAILABLE VIALS: 21

There is no way to be in contact with me before buying
After the payment I will send you an email about the delivery process;
there is no limit for sending it; it is worldwide

About the price, each vial is $5,000

Are you a patient??; check below

There are 2 vials for treatment and they are very rare

It has tested on Israeli patients and it works

I sell each for 25 thousand dollars; life is not cheap

Do not forget to fill all the fields

Available TREATMENT VIALS: 2/2

Important: DO NOT ORDER MORE THAN AVAILABILITY

Buy treatment vial; each 25000 $

There is no discount or shit like that; these vials are priceless and I can sell them more expensive than this but I wanted to put a fair price for it because I do nnot want to be a thief or an abuser

There is no paypal or check payment, just bitcoins. if you don't have bitcoins buy from a website like [redacted] or [redacted]

Do the payment and we will talk about the delivery

Scan the code or send the amount to the address that you get after filling the forms

IMPORTANT: THERE IS NO REFUND; FILL THE ADDRESS AND EMAIL VERY CAREFULLY

Important: DO NOT ORDER MORE THAN AVAILABILITY

THE OT LONG GAME

Operational technology (OT) encompasses the hardware and software used to control physical devices, processes and infrastructure that run cities and mass-scale industries. If successful, an OT hacker can disrupt water supplies, traffic signals, air controls, and more critical systems.

Because most OT systems are highly customized and proprietary, they are more difficult to hack, requiring means and motive over a longer period of time. Because of this, exposing vulnerabilities, even in routine testing, is important. The longer vulnerabilities go undetected, the more likely it is that a bad actor can access sensitive data or plan a more coordinated attack in the long term.

This begs the question: Who has the time, money or incentive to do this? The structure of the Dark Web offers sophisticated actors in big-stakes crime with access to intelligence and recruitment. Though less evident on the surface, the connection between increasingly targeted attacks and the Dark Web needs to be better understood — and more heavily investigated.

One of the most famous OT attacks dates back a decade, when the Stuxnet computer worm successfully targeted the PLCs (programmable logic controllers) connected to Iran's uranium enrichment facility, destroying centrifuges used for its nuclear program. As the first publicly known example of a virus being used to attack industrial machinery, many researchers and ethical hackers have studied it and, in retrospect, found vulnerability gaps that could have been closed before any damage was done. The question for security experts today is not if there are vulnerabilities, but how they are exploited to accumulate data about their organizations. **What information has been exposed, who is collecting it, and how is it being used?**

Can security experts and government officials expose the bad actors lurking in the shadows ready to strike at the most opportune moment?

OT attacks are not limited to television dramas and historic incidents like the Stuxnet worm. Just last spring, in 2020, the Trustwave SpiderLabs team published an advisory exposing two vulnerabilities in Schneider Electric PLC controller software and hardware that contained the potential for control-plane level attacks. Though a patch was successfully deployed to correct these issues, additional precautions were recommended, such as integrity checks when transferring applications as well as both machine and network hardening.

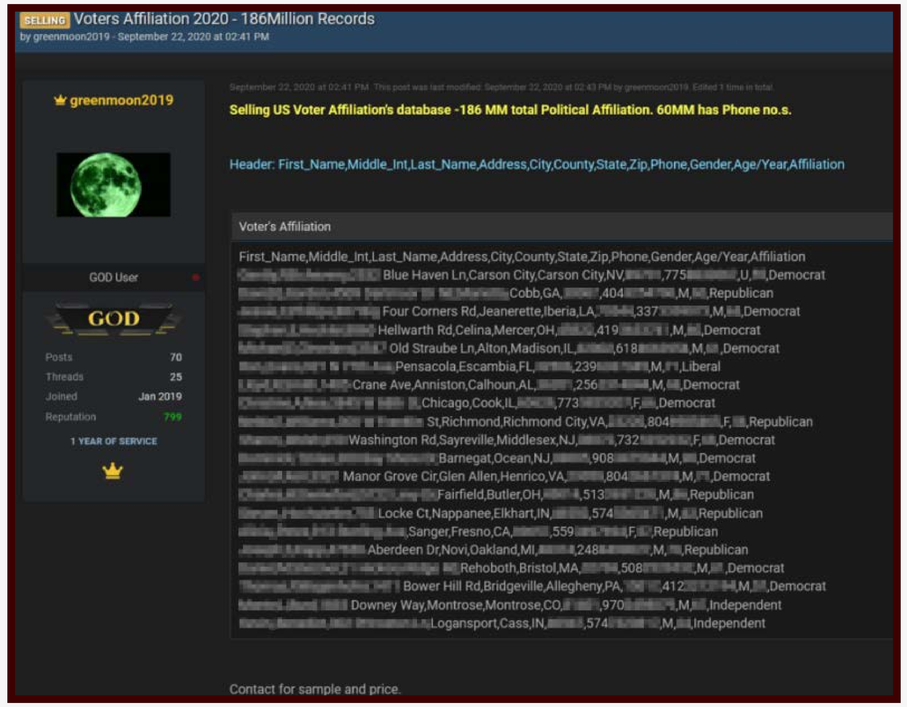
Managing privilege levels and increasing password complexity may seem like standard operating procedure, but these are important reminders, nonetheless. Unfortunately, as new brute-force attacks continue to be uncovered, even complex passwords can be hashed and obtained for full controller application privileges. If bartered on the Dark Web, these passwords would not only be highly valuable but could subsequently spread to a wider group of motivated bad actors.

Trustwave SpiderLabs discovered three additional vulnerabilities* on Schneider Electric software in the second half of 2020 alone, including ones that enabled application download from the M221 controller. Security flaws such as these could allow a bad actor to access controls and perform remote reconnaissance, gathering information for a future attack. Because the pool of victims is so widespread, the potential for significantly greater consequences than a single isolated network access instance is likely.

GEOPOLITICAL INTERFERENCE

When it comes to operational technology, nation-state actors are on the rise — and are using the infrastructure of the Dark Web to get ahead. That's not the only form of attack that has found a home in the espionage toolkit, though. Whenever geopolitical tensions in the world come to a head, there are corresponding activities on the Dark Web in which cybercriminals amplify desired outcomes as a form of patriotism to their state. And even in instances where geopolitical outcomes are not formally orchestrated, access to political records provides fodder for scams, disinformation campaigns and more.

During the 2020 U.S. elections, for example, the Trustwave SpiderLabs team discovered massive databases containing detailed information about U.S. voters and consumers for sale on several hacker forums. Both were noteworthy not only for their scale — 186 million records and 245 million records, respectively — but also what they symbolized: the increased capacity for data that is either publicly available or previously leaked to be aggregated and shared at strategic moments, allowing for both convenient access and maximum criminal impact.



The sale of the election data could have accelerated disinformation campaigns, potentially affecting every registered voter in the United States, without the hassle of mining data from cumbersome state records and correlating it with personal data from other sites.

With 400 potential data points on each individual record, the datasets paint a grim picture of complete data's profitability. The total value of the crypto wallet used to collect money from the sale of these consumer data records accrued $100 million in five months, though this likely includes revenue from other activities as well. These records were found on RaidForums.com, meaning interested buyers don't even need to visit the Dark Web to get in on the spoils; they existed in plain sight on the world wide web.

PUBLIC AND PRIVATE SECTOR IMPACT

When capitalist-fueled enterprise data is mixed with voter information, espionage isn't far from one's mind. Consider the implications of the recent SolarWinds Orion breach, for example. Although researchers continue to identify new information about the attack, it was considered the largest breach in history until the recently discovered Microsoft Exchange Server zero-day vulnerabilities, which are thought to be an even larger event. Reaching government stakeholders through major tech players like Microsoft and Cisco, the efforts show how vulnerabilities can compound over time.

The suspected Russian-backed masterminds behind the SolarWinds breach bypassed logins, outmaneuvered alert systems, and remained undetected for 15 at least months. The cybercriminals initially stayed dormant, implanting information in the source code, unbeknownst to the software developers. As of this publication, 18,000 organizations (government entities making up nearly 20% of the total) have been affected. The stolen data is available on the Dark Web, selling for up to $500,000 per list.

```
Happy new year!
Welcome to solarleaks.net (mirror: 5bpasg2kotxllmzsv6swwydbojnfuvfb7d6363pwe5wrzhjyn2ptvdqd.onion)

We are putting data found during our recent adventure for sale.

[Microsoft Windows (partial) source code and various Microsoft repositories]
price: 600,000 USD
data: msft.tgz.enc (2.6G)
link: https://mega.nz/file/1ehgSSpD#nrtzQwh-qyCaUHBXo2qQ1dNbWiyVHCvg8J0As8VjrX0

[Cisco multiple products source code + internal bugtracker dump]
price: 500,000 USD
data: csco.tgz.enc (1.7G)
link: https://mega.nz/file/sSgQmJLT#NqaaYXsFkASwAc51lcjBnWjP4zrbqiN-XQ7GVZGbL_o

[SolarWinds products source code (all including Orion) + customer portal dump]
price: 250,000 USD
data: swi.tgz.enc (612M)
link: https://mega.nz/file/xawhBQgJ#f3X61PORF16wh-O9GiNVMVDZ6rxRKX64_XVR5y9KpFM

[FireEye private redteam tools, source code, binaries and documentation]
price: 50,000 USD
data: feye.tgz.enc (39M)
link: https://mega.nz/file/hOBnVYjL#l3qojAvaFWtYtcB3vX4ZABG3tBLGyhJarBBbYaHnM-0

[More to come in the next weeks]

ALL LEAKED DATA FOR 1,000,000 USD (+ bonus)

Data is encrypted with strong key.
Serious buyers only: solarleaks@protonmail.com

- -
Q: Is this really happening? Can you provide proof?
A: Yes and yes.

Q: Why no more details?
A: We aren't fully done yet and we want to preserve the most of our current access. Consider this a first batch.

Q: I'm [vendor] and want my data back?
A: Talk to us.

Q: Why not leak it for free?
A: Nothing comes free in this world.

Q: How to buy?
A: Contact us for more information.
```

In an ingenious yet frightening move, the bad actors attached their malware to a security patch released to all Orion users. The magnitude of this rollout — at the enterprise level — sets a new precedent for hijacking supply chain software to carry forth the plans of bad actors. Positioned for the most massive impact, these criminals have no limits in their scope and continually adapt their offensive attacks.

A Microsoft report in early March of 2020, indicated that the named Microsoft Exchange zero-day vulnerabilities were being exploited by a new threat actor group Microsoft named HAFNIUM. According to Microsoft, HAFNIUM is a group assessed to be state-sponsored and operating out of China, based on observed victimology, tactics and procedures.

The scope of these attacks was reported by cybersecurity journalist Brian Krebs to be more widespread – at least 30,000 organizations across the United States and 100,000 organizations globally could be affected. Threat actors outside of HAFNIUM are also attempting to exploit the zero-day vulnerabilities. At the time of this writing, the investigations into the attack scope are ongoing, and Microsoft has not yet confirmed the full scope.

SUPPLY CHAIN ATTACKS

In the aftermath of SolarWinds, we see yet another reminder of the need for compliance and the cost of doing business today. Are your suppliers following the highest security frameworks? It's a snowball effect of catastrophic impact: with millions of suppliers affected and millions of additional suppliers connected to them, the attacker continues to infiltrate deeper into an ecosystem and all of its nodes. It's not enough to be confident your own security best practices are in place. The reality is vendors will need to go above and beyond standard procedures to show their awareness and responsiveness to future attacks of this nature. It's not a matter of if they're coming but when.

WHEN TIME IS NOT ON OUR SIDE

280 days | The average length of time it takes to identify and contain a breach*

Though the average time to discover a breach is decreasing overall, thanks to modern detection and response technologies and industry expertise, sophisticated attacks can take longer than ever to identify and mitigate. Unknown exploits, new tools, and new strains of malware can extend the length of time that elapses prior to discovering the presence of bad actors and malicious activity, let alone respond and effectively contain the threat.

The Inner Workings of the Dark Web

In the original Underground Economy publication, we examined the Dark Web's organizational structures and norms, its economic underpinnings and market forces, and how members get paid. Below, we'll elaborate on new trends and tactics in these areas.

THE CURRENCY OF DATA

Though every cybercriminal is different and runs their business accordingly, there has been a rise in self-identified data traders: those who buy and sell stolen data to be added to mega databases. On closed, vetted forums, this can be a full-time profession.

Similar to the gig economy, a bad actor determines the amount of time and skill to dedicate to each transaction, and much like the stock market, they weigh a myriad of considerations when deciding the right moment to buy or sell their data.

For example, after securing credentials of tens of thousands of residents in a particular geographic market, a data trader in this fictitious scenario could choose to sell these credentials piecemeal or seek opportunities to connect them to other datasets that may make the offer more enticing. Could healthcare records be parsed for extortion based on the sensitive nature of a diagnosis, or is it best to sell them quickly and turn a profit regardless of the details within? Trial and error are expected, and the Dark Web — with its slew of private messages — is the perfect place to test out demand for whatever data becomes available.

How is data valued, though? Let's outline a few scenarios:

- **Credit card information.** Much of this is done as a full-time profession for hackers to monetize through direct purchase and money laundering schemes, gaining access to e-commerce websites by compromising the client or server machine to retrieve credit card data.
- **Email addresses.** Email hacking services use automation to attempt billions of combinations to uncover valid, active emails, which, when sold in high volume, bring a premium price. Emails are batch sold to spammers where they are monetized through tactics like ransomware, coupon scams and more.
- **Credentials.** Hackers begin with poorly secured websites from small businesses (say, for example, your neighborhood pet store) to gain access to username and password combinations. Because many people use the same credentials across multiple sites, hackers then use automation to direct large-scale login requests against major websites, discovering matches for more lucrative credentials, like the victim's bank. This funnel — called credential stuffing — is becoming increasingly common. When they overlap with employee credentials in the era of remote work, the price tag for a sale on the Dark Web is much higher—and the business impact much more noteworthy.
- **Personally identifiable information (PII).** Lists that include first and last name, address, and sensitive information like mortgage lenders or health records are valuable for many reasons, not least of which being extortion. More complete records also enable targeted attacks against companies, executives, and other notable persons.

INFRASTRUCTURE BUILT TO BE RESILIENT

A large community built by technical people who know how to make money is self-sustaining. Originally created within academia on the premise of having the freedom to browse and communicate anonymously and without fear of being tracked online, the Dark Web has since evolved from there with government investments into a secure network (Tor) * for safer intelligence.

Since then, however, the Dark Web has evolved into a safe haven for criminals. With tens of thousands of contributors and dozens of forums (many of which are vetted and capped to maintain quality and privacy, due to the largely illicit nature of the exchanges), everything from drugs and ammunition to discounted (stolen) gift cards are available for purchase. You won't find much intelligence on hacking in the public forums; however, malware development, botnets, and exploits are reserved to the qualified few.

The infrastructure rotates its information and members across redundant platforms, and as the saying goes, when you cut off the head of one snake, five more grow. If one server or website is taken down, several more go up in its place. Like all organized crime, it will always exist in cyber society in some way or another. Even so, the Dark Web cannot be treated as a necessary evil; its exploits must be matched with innovative and dynamic counter-responses. This is an investment all stakeholders must agree to uphold, as criminals get better at exchanging information and monetizing their activity.

* The onion router (Tor) is a technology that enables people to access online services and browse the internet without revealing their identities. The Tor networks are made up of thousands of servers located around the globe.

The Double Agent: Underground, Under Cover

Thinking like a hacker is a crucial part of security expertise. It's in the mind of the highly motivated, resourceful and creative computer scientist, social engineer or transactions officer where we find the most promising tools to anticipate and defend against attacks and limit the severity of possible outcomes.

GETTING BEHIND THE OFFER

In most cases, finding a post on a Dark Web forum that matches client criteria or a lead under investigation is only the first step in the long process threat hunters use to uncover meaningful findings. Often, a post describes a service without detailing the product itself; and, since all messages are private and initiated behind an alias, intercepting direct communication is difficult for investigators. Ethical hackers embedded into open or closed forums, however, can potentially begin a line of questioning via private messages in order to gather valuable information on the nature of an offer and its going rate.

TRACKING THE MONEY

Traditional money laundering techniques have found creative strongholds via digital channels and third party sharing economy apps like Uber and AirBnB, using cryptocurrency to fuel payments. While droppers and mixers are meant to create confusion and noise in the time it takes authorities to notice any suspicious activity, Bitcoin and others can be openly tracked via online ledger. Technological innovation provides transparency for transactional methods that reign on the Dark Web, but the trail is becoming increasingly hard to follow.

METHODS FOR DARK WEB RESEARCH

Dark Web research and proactive threat hunting are labor and skill intensive, seeking to match the ingenuity of the criminals themselves. Though more security firms now offer Dark Web monitoring as part of their broader threat hunting services, the quality varies greatly. Here are some examples of what to look for in a reputable third-party provider to help prevent your company's data from getting ensnared in malicious activity on the Dark Web.

1. Learn about what cybercriminals do, tracking trends and activity on the Dark Web — and off of it.

2. Monitor information on the Dark Web, including company domain names, email addresses, facility references and the names and information of executives, noting best practices for automation where applicable. Testing through social engineering helps expose weak links at the employee level that can then be investigated on the Dark Web. Security experts can potentially initiate conversations with bad actors for more detailed transactional data as appropriate, based on the evidence discovered while monitoring.

3. Share intelligence through advisories to make the entire security community smarter — and businesses more informed.

4. Create tools to detect exploits and block attacks at their point of origin, going beyond antivirus and firewall protection. Routinely test environments based both on what has already been discovered as well as current trends.

5. Block access to phishing domains and share them as they become known, so that unintended compromises don't take place where system users are most susceptible.

HACKER CHATS: DARK WEB LINGO

If you want to think like a hacker, you've got to talk the talk. Here are some terms to get you started.

Chommer: a forum member who uses multiple accounts — an action that can lead to being banned from the community

Doxing: Revealing contact information of a member as punishment for breaking forum rules, thereby exposing them to potential legal ramifications

Drive-in: Using stolen credit cards for profit

FUD: Fully undetectable (by AV software); clean malware or exploits for purchase

Full CC: Stolen credit card with complete information

Mats: Materials (stolen goods, like credit cards)

Pick up: a money withdrawal for laundering

Piercing: The service of illegally looking up information on an individual

Ripper: Term used to flag when someone has been doxed from community

Toad: slang for Jabber, a secure chat application commonly used by cybercriminals

Unsaturated: Limited sharing / prior exposure of goods (to other sellers)

A Rise in Sophisticated Attacks: What they look like today

There are still ample examples of petty theft, job postings for simple tasks, and threads on emerging skills and hacking techniques on the Dark Web. Meanwhile, cybercrime continues evolving to cover its tracks, requiring numerous players and ensuring monies or goods exchange multiple hands. What can be seen on the pages of the Dark Web show only piecemeal tactics of much more complex, interdependent schemes.

The Dark Web can feel mysterious and even a bit exciting to those interested in the world of technology, but its impact goes far beyond what is viewable on its .onion domains (Tor). Cybercriminals that conduct targeted attacks, especially advanced persistent threats (APTs) and nation-state actors, continue to demonstrate an incredibly high level of sophistication. Like the GoldenSpy malware, mitigated in the spring of 2020, the SolarWinds vulnerabilities, or the recent Microsoft Exchange Server vulnerabilities, the development of teams of professionals that aren't likely to be actively posting on forums or making requests continues to grow.

There is another, arguably more prominent, group of bad actors on the Dark Web that also monitors activity in an attempt to stay one step ahead of the security teams protecting against them. These groups are not motivated by quick profits or the strategic bartering of stolen data or goods; however, they are significantly more dangerous and their motives more insidious than other bad actors. Nation-state intelligence operatives and cybercriminals now circumvent the Dark Web, using it only sparingly to attain minor pieces of a more significant and potentially more dangerous puzzle.

Though the Dark Web continues to thrive as an underground source of community, information sharing, research and dubious payments, all of this is just the tip of the iceberg. The players who rule over the underground economy are now maneuvering boldly above ground as well.

CLOSE-UP: TRUSTWAVE SPIDERLABS

Trustwave SpiderLabs

The Trustwave SpiderLabs team has published over one hundred advisories, finding vulnerabilities in everything from coffee makers to proprietary software. Beyond scheduled activity and rigorous client investigations, monthly discoveries are a combination of individual curiosity, client requests or managed services. If a client purchases a new furnace, for example, SpiderLabs team members will attempt to hack the connected app — in addition to their existing work demands — and share their learnings along the way.

Constantly busy investigating new cyber threats, SpiderLabs team members proactively attempt to hack new products and services (like the Magic Home Pro mobile application and the security advisory that followed) before any suspicious activity has surfaced— and they frequently succeed. This is part of an ongoing, cyclical process of alerting companies to security gaps before a bad actor exploits them, then sharing the information publicly so that other security experts can be more responsive to these gaps relative to their own business and IT environments.

RESPONSIBLE DISCLOSURE

The process of sharing discoveries to the public surrounding a successful breach or an exposed vulnerability is called responsible disclosure. SpiderLabs experts begin with private outreach to the vendor who owns the affected product. In most cases, Trustwave will work closely with an in-house team to better understand the details of the security gap. When the company creates a subsequent patch, the SpiderLabs team will offer its help in testing it to ensure the vulnerability has been properly fixed. Only after the patch has been released, will they post the findings publicly.

Because of the nature of cybercrime, exceptions may be required. Depending on how responsive a company is to a security notice, and the sensitivity of the discovery, the following etiquette is advised:

1. The vendor will be given 14 days from the date of contact for an initial response. Should no contact occur by the end of 14 days, Trustwave SpiderLabs will evaluate the risk to its clients and may decide to disclose the vulnerability to them, at a minimum.
2. Trustwave SpiderLabs will provide a best effort to honor requests from the vendor for additional information or help in reproducing the vulnerability. This will include providing configuration details and the scenario in which the vulnerability was discovered.
3. The vendor is responsible for providing regular status updates (regarding the resolution of the vulnerability). If the vendor discontinues communication at any stage of the process for more than 30 days after date of contact, Trustwave SpiderLabs will view the vendor as non-responsive and will consider public disclosure.
4. The vendor is encouraged to provide proper credit to Trustwave and to the researcher responsible for discovering the vulnerability. Suggested (minimal) credit would be: "Credit to [researcher name] from the SpiderLabs team at Trustwave for disclosing the vulnerability to [vendor name]."
5. The vendor is encouraged to coordinate a joint public release/disclosure with Trustwave SpiderLabs so that the announcement of the vulnerability and its resolution can be made simultaneously.
6. The vendor will be given a maximum of 90 days after the date of contact to release a patch. After 90 days, Trustwave SpiderLabs will consider public disclosure.
7. If a third party publicly discloses the vulnerability during this process, disclosure will be considered to be public, and Trustwave SpiderLabs will work with the vendor for immediate disclosure.
8. If the vulnerability is being actively exploited in the wild, Trustwave SpiderLabs will work with the vendor on an escalated disclosure timeline. This could potentially take place less than seven days after the initial contact date if the exploitation is experienced on a wide and public scale.
9. Proof of concept code or the technical explanation of a vulnerability's exploitation that is rated critical may be withheld for up to 14 days after public disclosure to allow time for organizations to protect themselves.

This policy takes into account the speed at which bad actors can work and the ripple effect that can follow if a vulnerability is left unaddressed for any period of time, let alone a prolonged one.

What's Next? Uniting Forces Against Cybercrime

Security experts alone cannot keep cybercriminals from exploiting their victims; they instead work tirelessly to mitigate damage and remain aware of newly developing tactics as they emerge. Governments and law enforcement officials—often working in tandem with private sector organizations—also play a critical role. These groups amplify the guidance shared by security experts, take actions, and create counter-response strategies to Dark Web activity. Equipped to catch criminals and shut down what are often internationally operated schemes, these groups provide critical resources such as making payments, summoning extradition, and luring criminals to target destinations to shut down crime rings and high-profile actors.

Additional reading: the 2021 Emotet botnet takedown by a coalition of international law enforcement agencies, including the United States, Canada, the United Kingdom and others

For decades, the Dark Web has been largely left to its own devices, sheltered in a community free from major repercussions beyond its own rules and regulations. A member would be far more likely to be doxed as a form of punishment, for example, than it would to be exposed and prosecuted for criminal activity outside of the Dark Web itself.

This is changing, however; in January 2021, Europol and its newly established dedicated Dark Web Team at the Europol Cybercrime Centre (EC3) took the world's largest illegal marketplace, DarkMarket, offline in a cross-border collaborative effort between Germany, Australia, Denmark, Moldova, Ukraine, the United Kingdom (the National Crime Agency), and the USA (DEA, FBI, and IRS). Though the rise and fall of Dark Web sites — much like organized crime rings in the traditional sense — is a game of cat and mouse; international orchestration and increased oversight show that the Dark Web's capabilities are being recognized more than ever.

A mature underground market system both benefits savvy grifters and advances the efforts of nation state-sponsored crime. Today, academia, law enforcement, and corporate security experts must be better aligned to minimize the impact of highly skilled cybercriminals. Innovators like the DarkTower forensics team at University of Alabama Birmingham apply the talents of industry veterans and promising students alike to map connections between cybercrime, financial crime, fraud, and terrorist activity using forensic intelligence. Banks rely on their work, federal agencies and law enforcement utilize their findings, and the talent pool for qualified security experts grows alongside its program. More of this is needed, from recruitment to focused collaboration, to keep pace with the supply and demand for talent and skill reflected in the underground economy of the Dark Web.

DARKMARKET BY THE NUMBERS

1. 500k users
2. 2,400 sellers
3. 320k transactions
4. Nearly $170M (140M euro) exchanged

Closing Thoughts

Companies today must be vigilant. As we've seen in the cases of GoldenSpy, SolarWinds and more, malware can be cleverly hidden in any software, regardless of its source or supposed legitimacy. At the same time, entities on the Dark Web are pooling data from breaches over time, connecting the dots between isolated instances of petty theft and bigger schemes to create opportunities for more orchestrated — and far-reaching — malicious intent.

It will take matched coordination, incentivization and motive to keep up with bad actors on and off the Dark Web, and the security budgets of corporations, government agencies, and software providers should reflect this collective responsibility. In a world where everything's connected, the players who are monitoring these connections and being the connectors of information in turn — on and off the Dark Web — will be the ones best poised to respond.

Additional resources

GOLDENSPY MALWARE

- Chapter One: Overview
- Chapter Two: The Uninstaller
- Chapter Three: The New and Improved Uninstaller
- Chapter Four: GoldenHelper
- The Golden Tax Department and the Emergence of GoldenSpy Malware
- [Research Report] The Golden Tax Department and the Emergence of GoldenSpy Malware
- [Webinar-on-Demand] GoldenSpy: Hunting Threats and Understanding Your Risks

SOLARWINDS ORION COMPROMISE

- Trustwave's Action Response
- Full System Control with New SolarWinds Orion-based and Serv-U FTP Vulnerabilities
- [Webinar-on-Demand] Overview of New SolarWinds Vulnerabilities Discovered by Trustwave SpiderLabs

MICROSOFT EXCHANGE SERVER ZERO-DAY VULNERABILITIES

- Trustwave's Action Response to the Microsoft Exchange Server Zero-Day Vulnerabilities and Attacks
- HAFNIUM, China Chopper and ASP.NET Runtime

SCHNEIDER VULNERABILITIES

- Part One
- Part Two
- Part Three

COVID-19 SCAMS

- BEC scams
- Vaccine scams and more

PHISHING

- Cloud platform vulnerabilities
- Google Play card scam (see also, ransomware)
- Using Google Firebase Storage

SPAM

- Evasive URLs

HACKING (GENERAL)

- ATM hacks
- Online coupons

Trustwave®

trustwave.com