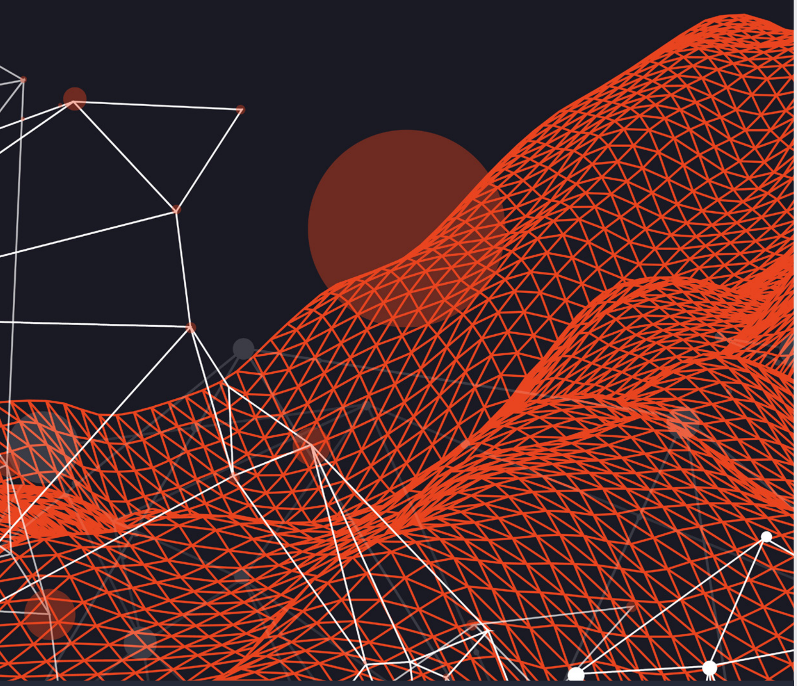
SEARCHLIGHT.
CYBER

USING THE DARK WEB
FOR PRE-ATTACK INTELLIGENCE

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS



SEARCHLIGHT.
CYBER

Searchlight Cyber provides organizations with relevant and actionable dark web threat intelligence, to help them identify and prevent criminal activity. Founded in 2017 with a mission to stop criminals acting with impunity on the dark web, we have been involved in some of the world's largest dark web investigations and have the most comprehensive dataset based on proprietary techniques and ground-breaking academic research. Today we help government and law enforcement, enterprises, and managed security services providers around the world to illuminate deep and dark web threats and prevent attacks.

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

CONTENTS

INTRODUCTION

To date, when cybersecurity companies have discussed “the anatomy of a cyberattack” they have focused on the sequence of events and the actions attackers take to execute their attack once they are on the network. However, this is not the whole picture.

A cyberattack doesn’t start on the network, it starts weeks, months or even years before as threat actors do their due diligence on their target, plan their path of attack, coordinate their efforts, and purchase the tools, credentials or access they need to execute their operations.

SEARCHLIGHT IN NUMBERS

VISIBILITY INTO
830,000+
LIVE AND HISTORIC DARK WEB SITES

90+
DARK WEB MARKETPLACES

70+
DARK WEB FORUMS

> **“A CYBERATTACK DOESN’T START ON THE NETWORK, IT STARTS WEEKS, MONTHS OR EVEN YEARS BEFORE.**

Understanding how threat actors maneuver their way through an organization’s infrastructure is valuable for informing network security and incident readiness but it does little to help security teams prevent their network being breached in the first place. Organizations need threat intelligence on cybercriminal pre-attack activity in order to take action to stop (rather than just mitage) a breach.

Threat actors’ reconnaissance largely takes place on the deep and dark web, where they believe they can act with impunity, out of reach of cybersecurity teams and law enforcement. Dark web intelligence is organizations’ best chance to undermine that activity, to arm themselves with the adversarial knowledge they need to pre-empt and prevent attacks, and reduce the impact and cost of cybercrime to their business.

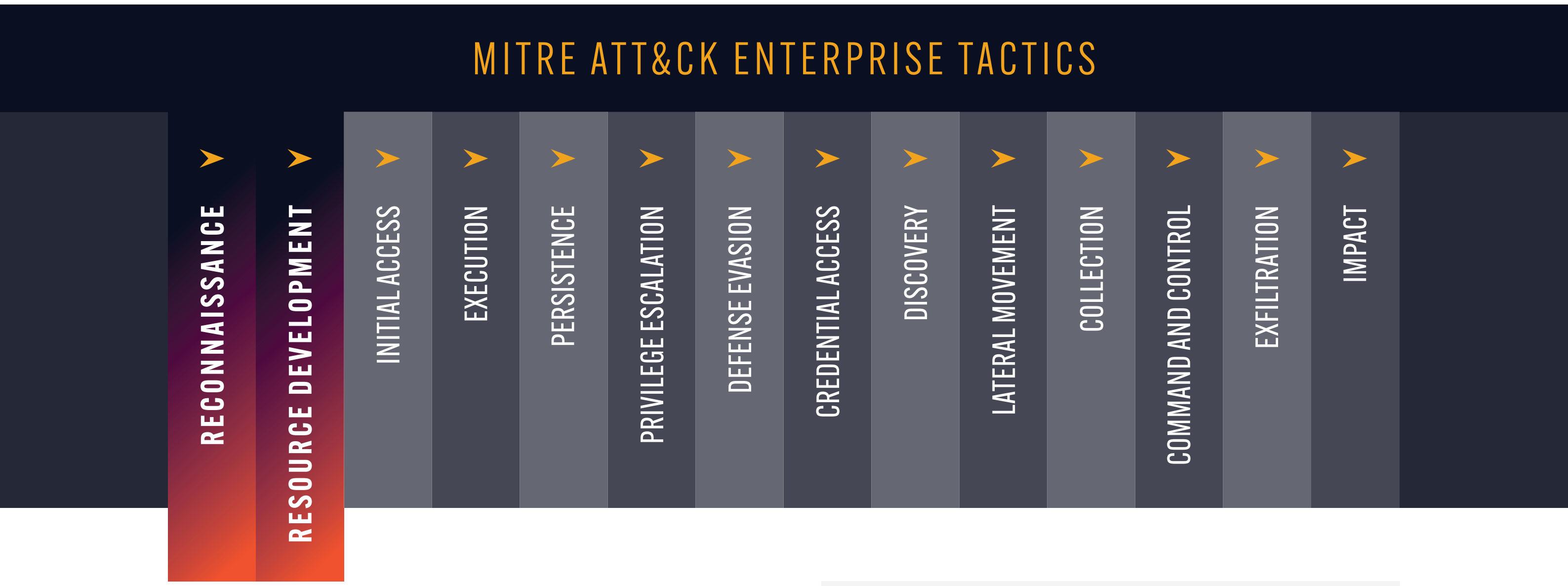
This report uses real deep and dark web intelligence from infamous cybersecurity incidents to demonstrate the red flags that could indicate an imminent threat to a company, and help them to adjust their security posture to prioritize likely attacks.

JIM SIMPSON
Director of Threat Intelligence,
Searchlight Cyber

DARK WEB INTELLIGENCE AND THE MITRE ATT&CK FRAMEWORK

The MITRE ATT&CK framework, a knowledge base of adversary Tactics, Techniques and Procedures (TTPs) based on real-world observations, is a popular tool for organizations creating threat models and methodologies to protect themselves from attacks. It is also useful for explaining where dark web intelligence fits in an organization's defenses.

The MITRE ATT&CK Enterprise Matrix[1] is a chain of actions that threat actors take to execute an attack on an organization's network, with the techniques they might use at each stage and recommendations for how organizations can defend themselves against each one.



MITRE ATT&CK ENTERPRISE TACTICS

RECONNAISSANCE

RESOURCE DEVELOPMENT

INITIAL ACCESS

EXECUTION

PERSISTENCE

PRIVILEGE ESCALATION

DEFENSE EVASION

CREDENTIAL ACCESS

DISCOVERY

LATERAL MOVEMENT

COLLECTION

COMMAND AND CONTROL

EXFILTRATION

IMPACT

The tactics we are most concerned with are Reconnaissance (TA0043)[2] and Resource Development (TA0042)[3], the two stages that are grouped by MITRE in the PRE Matrix[4]. These two tactics are significant because they are the only ones that focus on the period of time before the network is breached. I.e. this is the only point in which organizations have an opportunity to stop that from happening.

RECONNAISSANCE

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting, which may include details of the victim organization, infrastructure, or staff/personnel.

RESOURCE DEVELOPMENT

Focused on an adversary trying to establish resources they can use to support operations, including techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting.

As MITRE ATT&CK states, mitigating attacks at this stage can be challenging, "as they take place in a space outside of an enterprise's defenses and control". However, dark web intelligence gives organizations an opportunity to extend their view out beyond their organization and into the Reconnaissance and Resource Development stages. Armed with this intelligence, they can modify and enhance their defenses based on greater clarity of exactly who is planning to attack their organizations, and how they plan to do it.

GATHERING DARK WEB INTELLIGENCE ON THREAT ACTORS

Adversarial intelligence is key for organizations looking to gain the upper hand on their attackers while they are in the Reconnaissance and Resource Development phases.

These two case studies of LAPSUS$ and DarkSide - two notable threat clusters from the past few years - demonstrate what we can learn about the TTPs used by each group from dark web intelligence.

As the contrast between the two groups shows, while the impact on the business might be the same, there are substantial differences between how threat groups operate. Therefore, treating all threat actors as a like-for-like threat is a mistake, and dark intelligence is one way organizations can create a more reliable picture of the adversary.

> “
>
> **TREATING ALL THREAT ACTORS AS A LIKE-FOR-LIKE THREAT IS A MISTAKE, AND DARK INTELLIGENCE IS ONE WAY ORGANIZATIONS CAN CREATE A MORE RELIABLE PICTURE OF THE ADVERSARY.**

LAPSUS$

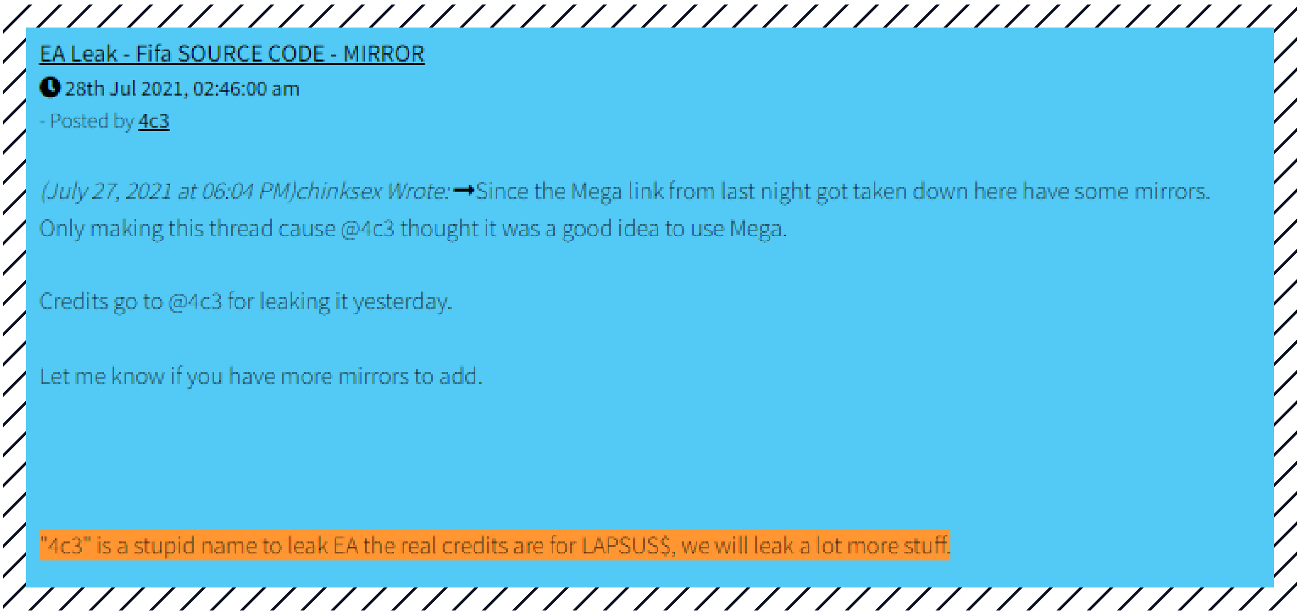
BACKGROUND

In December 2021, a new threat actor emerged, primarily targeting corporate and government entities in Portugal and Brazil. While attracting some attention, the group initially kept a fairly low profile before changing tact: moving into the data extortion scene, picking larger targets at increasing frequency, and becoming increasingly outspoken. While the group's activity declined after a number of arrests in March 2022, LAPSUS$ nevertheless became notable in its short tenure for the volume of its activity, its targets (which included Brazil's health ministry, Impresa, Claro, Samsung, and Nvidia), and its unique approach to communication.

Deep and dark web intelligence gives us insight into the group, its tactics, and its operations that were not widely known or reported at the time.

THE GROUP'S ORIGINS

While it was initially reported that LAPSUS$ began operations in December 2021 with an attack on Brazil's health ministry, dark web forum records show that the group was actually active for almost half a year prior to this attack. In June 2021, source code stolen from the games developer EA was listed for sale on the popular hacking and leaks site RaidForums by the username 4c3. This user later credited LAPSUS$ with the breach and promised they would be leaking more data soon **(Figure 1)**.



EA Leak - Fifa SOURCE CODE - MIRROR

🕒 28th Jul 2021, 02:46:00 am

- Posted by 4c3

(July 27, 2021 at 06:04 PM)chinksex Wrote:➞Since the Mega link from last night got taken down here have some mirrors. Only making this thread cause @4c3 thought it was a good idea to use Mega.

Credits go to @4c3 for leaking it yesterday.

Let me know if you have more mirrors to add.

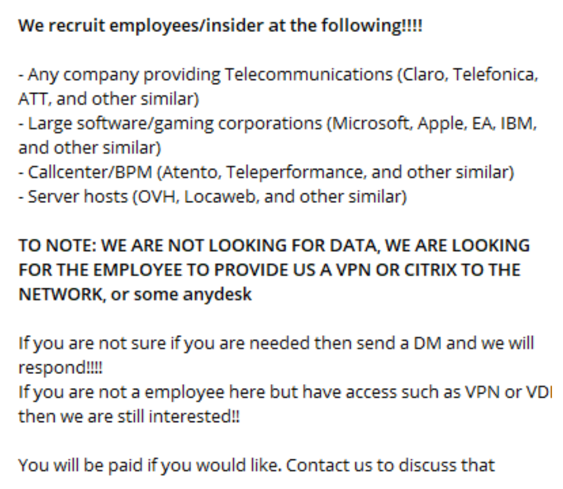
"4c3" is a stupid name to leak EA the real credits are for LAPSUS$, we will leak a lot more stuff.

FIGURE 1: 4C3 CREDITS LAPSUS$ WITH THE EA BREACH AND PROMISES MORE DATA.

ITS COMMUNICATIONS STRATEGY

The LAPSUS$ Telegram channel was created in December 2021, seemingly to amplify the Brazilian health ministry hack. This is notable for its divergence from other ransomware and threat actors, who tend to favor dark web sites to publicize their attacks. LAPSUS$ often used its Telegram channel to claim responsibility for attacks, for example, suggesting that it was responsible for an attack against Ubisoft by resharing a news story accompanied by a smirking emoji.

However, it also went further than most other threat actors - whose public communication would usually be limited to announcing, auctioning and sharing stolen data - by using its Telegram channel to crowdfund access to organizations. For example, putting out a recruitment call to malicious insiders at large telecommunication, software, call center, and server host firms **(Figure 2)**.



We recruit employees/insider at the following!!!!

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

You will be paid if you would like. Contact us to discuss that

FIGURE 2: A RECRUITMENT POST IN THE LAPSUS$ TELEGRAM CHANNEL.

While other actors might use similar tactics, this is typically done in a less conspicuous manner over private messages, not on a public Telegram channel with 47,000 subscribers and in full view of law enforcement and security researchers.

> **REPORTS THAT LAPSUS$ WAS A RANSOMWARE GANG WERE PROVED FALSE BY INSIGHT FROM ITS TELEGRAM CHANNEL. ASKED ABOUT THEIR TACTICS, LAPSUS$ STATED ON THEIR CHANNEL “WE SAID IT WAS A RANSOM, NOT A RANSOMWARE”.**

ITS TACTICS, TECHNIQUES AND PROCEDURES

Again, initial reports that LAPSUS$ was a ransomware gang were proved false by insight from its Telegram channel. Asked about their tactics, LAPSUS$ stated on their channel “we said it was a ransom, not a ransomWARE”. LAPSUS$ is subsequently best classified as a data extortion actor - one which breaches corporate networks, exfiltrates sensitive data and demands a ransom in return for not leaking the information online. There were also occasions where LAPSUS$ claimed to engage in data wiping against its targets, raising the stakes for the data’s return and thus the likelihood of ransoms being paid.

Dark web intelligence also sheds light on the mystery of how LAPSUS$ gained access to its victims’ networks in the first place, with forum posts and Telegram messages suggesting that the group purchased stolen logins and browser fingerprints from cybercrime markets such as Genesis. The EA hack relied on social engineering of staff in the company’s Slack channel, and its call for malicious insiders also indicates another potential path it utilized for attacks.

ITS CONFLICTS WITH OTHER THREAT ACTORS

Another distinguishing feature of LAPSUS$ was its readiness to make enemies with other threat actors. Although conflict within the cybercriminal underground is nothing new - groups regularly turn their hacking skills on their competitors - LAPSUS$ became embroiled in several disagreements that seemed particularly personal and contributed to its image as an impulsive group that cared little for the prevailing norms of the wider cybercrime community.

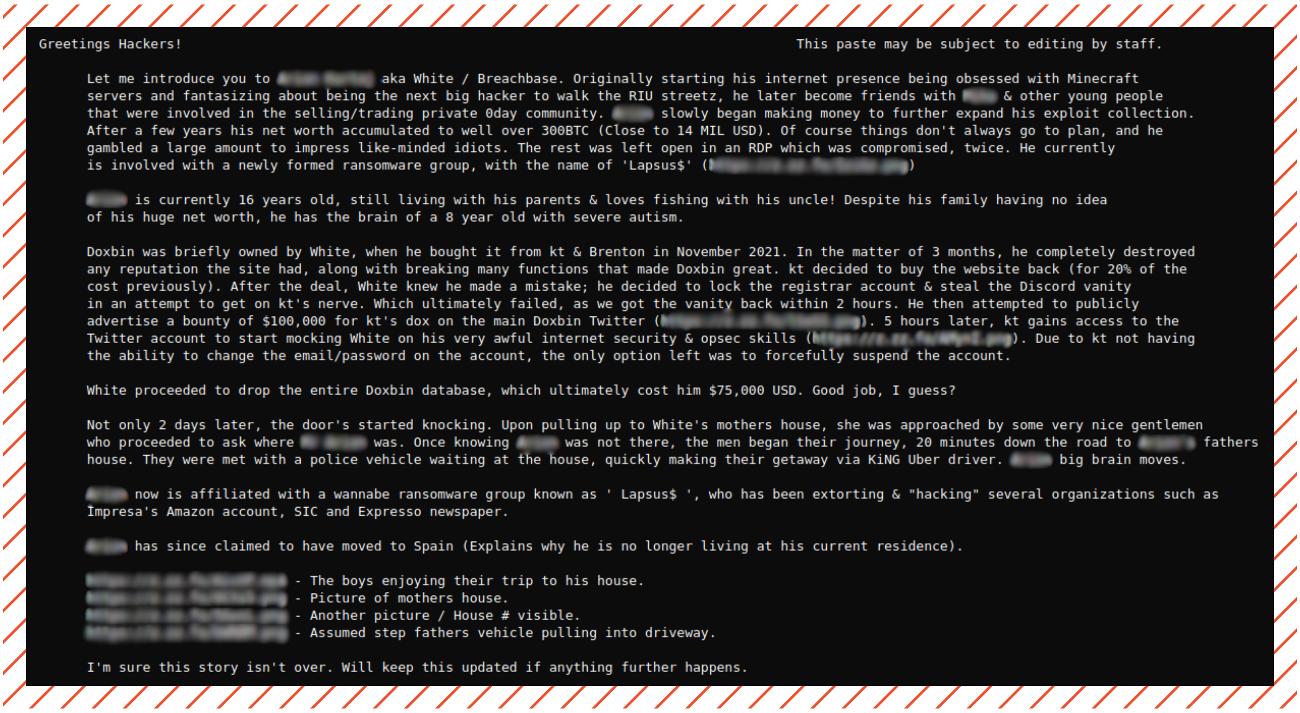
LAPSUS$ first displayed its appetite for disputes following the EA hack. An actor by the name of Leakbook, who had been active on RaidForums since 2018, dumped EA data in a post titled “FIFA 21 SOURCECODE + TOOLS” in June 2021. Analysis of forum posts between the two suggests the actors were at one point working together, with Leakbook acting as a seller of the FIFA source code on behalf of LAPSUS$’ alter ego 4c3.

This relationship quickly soured after 4c3 posted “EA News” the following month, announcing that they had breached EA and were in the process of trying to extract a ransom payment from the company.

In a follow-up post titled “The Biggest EA Data Leak”, Leakbook ridiculed 4c3 for failing to successfully extort EA, instead releasing the data for free. Leakbook made several other posts deriding 4c3/LAPSUS$’ handling of the situation, including leaking the ransom email allegedly sent to EA. LAPSUS$ members were dubbed by Leakbook and other RaidForums users as “skids” (short for “script kiddies”), a derogatory term for would-be hackers who lack actual programming expertise, instead relying on pre-written scripts.

THE IDENTITY OF THE HACKERS

These disputes resulted in information on the identity of one of the LAPSUS$ group hackers being leaked online. In January 2022, a post was made on Doxbin - a site used to release personal information about an individual - claiming that an affiliate of LAPSUS$ was a 16-year-old boy living in the UK **(Figure 3)**. The dox post accused the teenager - alias White - of buying and briefly owning the site Doxbin before selling it back to the original owners and leaking its database. This incident only came to light in March 2022, as the UK police arrested seven teenagers.



```
Greetings Hackers!                                                          This paste may be subject to editing by staff.

      Let me introduce you to [redacted] aka White / Breachbase. Originally starting his internet presence being obsessed with Minecraft
      servers and fantasizing about being the next big hacker to walk the RIU streetz, he later become friends with [redacted] & other young people
      that were involved in the selling/trading private 0day community. [redacted] slowly began making money to further expand his exploit collection.
      After a few years his net worth accumulated to well over 300BTC (Close to 14 MIL USD). Of course things don't always go to plan, and he
      gambled a large amount to impress like-minded idiots. The rest was left open in an RDP which was compromised, twice. He currently
      is involved with a newly formed ransomware group, with the name of 'Lapsus$' ([redacted])

      [redacted] is currently 16 years old, still living with his parents & loves fishing with his uncle! Despite his family having no idea
      of his huge net worth, he has the brain of a 8 year old with severe autism.

      Doxbin was briefly owned by White, when he bought it from kt & Brenton in November 2021. In the matter of 3 months, he completely destroyed
      any reputation the site had, along with breaking many functions that made Doxbin great. kt decided to buy the website back (for 20% of the
      cost previously). After the deal, White knew he made a mistake; he decided to lock the registrar account & steal the Discord vanity
      in an attempt to get on kt's nerve. Which ultimately failed, as we got the vanity back within 2 hours. He then attempted to publicly
      advertise a bounty of $100,000 for kt's dox on the main Doxbin Twitter ([redacted]). 5 hours later, kt gains access to the
      Twitter account to start mocking White on his very awful internet security & opsec skills ([redacted]). Due to kt not having
      the ability to change the email/password on the account, the only option left was to forcefully suspend the account.

      White proceeded to drop the entire Doxbin database, which ultimately cost him $75,000 USD. Good job, I guess?

      Not only 2 days later, the door's started knocking. Upon pulling up to White's mothers house, she was approached by some very nice gentlemen
      who proceeded to ask where [redacted] was. Once knowing [redacted] was not there, the men began their journey, 20 minutes down the road to [redacted] fathers
      house. They were met with a police vehicle waiting at the house, quickly making their getaway via KiNG Uber driver. [redacted] big brain moves.

      [redacted] now is affiliated with a wannabe ransomware group known as ' Lapsus$ ', who has been extorting & "hacking" several organizations such as
      Impresa's Amazon account, SIC and Expresso newspaper.

      [redacted] has since claimed to have moved to Spain (Explains why he is no longer living at his current residence).

      [redacted] - The boys enjoying their trip to his house.
      [redacted] - Picture of mothers house.
      [redacted] - Another picture / House # visible.
      [redacted] - Assumed step fathers vehicle pulling into driveway.

      I'm sure this story isn't over. Will keep this updated if anything further happens.
```

FIGURE 3: A POST IN DOXBIN ON JANUARY 8, 2022 DOXING LAPSUS$ MEMBER WHITE, A 16 YEAR OLD FROM THE UK.

DARKSIDE

BACKGROUND

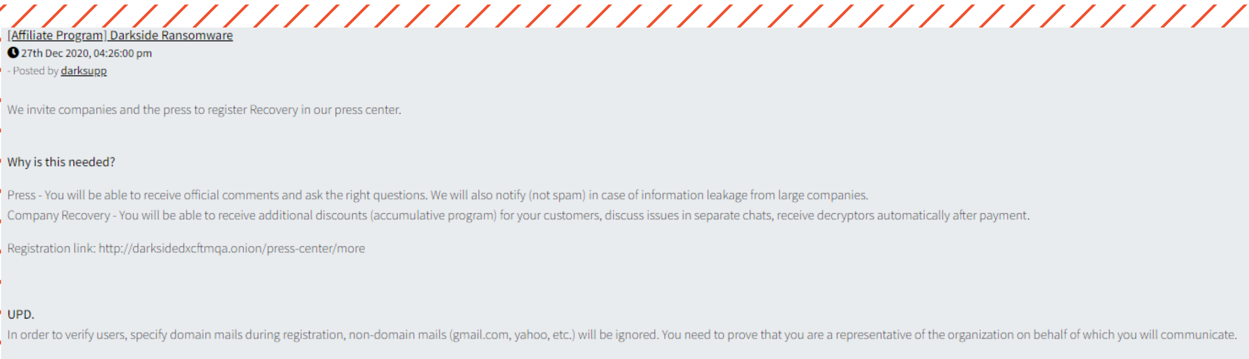
DarkSide was a Ransomware-as-a-Service (RaaS) group that amassed tens of victims in the period in which it operated, but is most infamous for being responsible for the Colonial Pipeline attack in May 2021. The group launched initially in August 2020 with its own ransomware venture, using a variant that shared code with REvil. In November 2020 the group began an affiliate program, offering its ransomware to third-party actors in return for a share of the profits. The DarkSide leak site's .onion address closed in May 2021, shortly after the Colonial Pipeline attack, most likely in response to attention from law enforcement.

DarkSide makes an interesting comparison with LAPSUS$. While the groups share some similarities - they both focused on "big game hunting" and their network intrusion tactics are similar, with DarkSide also reportedly[5] utilizing VPN access through leaked passwords - their dark web presence is a stark contrast. Once again, dark web intelligence can tell us a lot about how the DarkSide group functioned and organized itself.

> **WHILE THE LAPSUS$ AND DARKSIDE GROUPS SHARE SOME SIMILARITIES THEIR DARK WEB PRESENCE IS A STARK CONTRAST.**

ITS COMMUNICATIONS STRATEGY

Compared to LAPSUS$, DarkSide is more in line with traditional threat actors' communication methods, utilizing its own dark web leak site and the Russian hacking forums XSS and Exploit, where it posted under the username darksupp. One indication that DarkSide was a more professional outfit is the "press center" it established to share information with journalists and the organizations impacted by its operations, which it can be seen advertising in **Figure 4**.



[Affiliate Program] Darkside Ransomware
27th Dec 2020, 04:26:00 pm
- Posted by darksupp

We invite companies and the press to register Recovery in our press center.

Why is this needed?

Press - You will be able to receive official comments and ask the right questions. We will also notify (not spam) in case of information leakage from large companies.
Company Recovery - You will be able to receive additional discounts (accumulative program) for your customers, discuss issues in separate chats, receive decryptors automatically after payment.

Registration link: http://darksidedxcftmqa.onion/press-center/more

UPD.
In order to verify users, specify domain mails during registration, non-domain mails (gmail.com, yahoo, etc.) will be ignored. You need to prove that you are a representative of the organization on behalf of which you will communicate.

FIGURE 4: DARKSIDE ENCOURAGES COMPANIES AND JOURNALISTS TO REGISTER FOR ITS "PRESS CENTER".

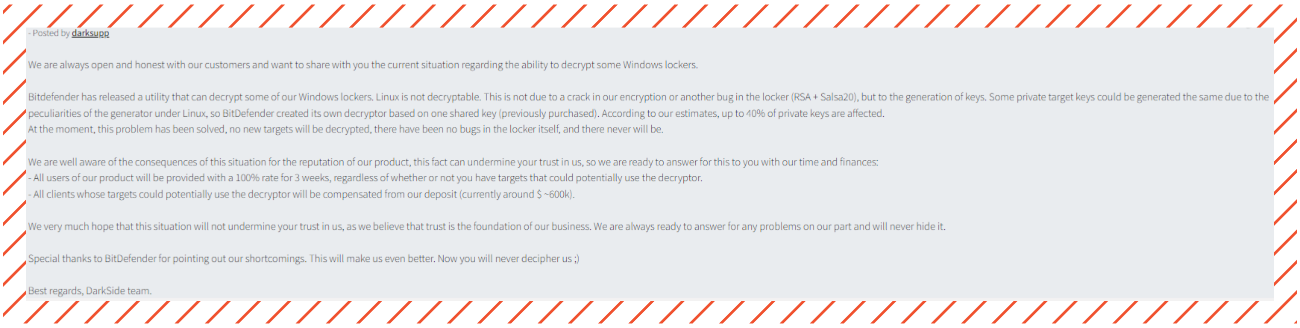
ITS AFFILIATE PROGRAM

The dark web communication between DarkSide and its affiliates also tells us a lot about the group.

Firstly, DarkSide set out rules for its affiliates, stating that it targets only big companies and forbidding its partners from targeting certain industries, including healthcare, funeral services, education, public sector and non-profits, for "ethical" reasons. Affiliates were also vetted and were unable to target organizations in the Commonwealth of Independent States (CIS) - which includes Russia and many former Soviet Union countries.

Secondly, the posts DarkSide shared for its affiliates once again demonstrate the professionalization of the operation. Take, for example, these posts communicating an update to its product following a decryptor released by Bitdefender that compromised some of the group's operations.

On January 12, 2021 the darksupp alias provided a thorough overview of the situation to reassure its customers that it is trustworthy **(Figure 5)**.



- Posted by darksupp

We are always open and honest with our customers and want to share with you the current situation regarding the ability to decrypt some Windows lockers.

Bitdefender has released a utility that can decrypt some of our Windows lockers. Linux is not decryptable. This is not due to a crack in our encryption or another bug in the locker (RSA + Salsa20), but to the generation of keys. Some private target keys could be generated the same due to the peculiarities of the generator under Linux, so BitDefender created its own decryptor based on one shared key (previously purchased). According to our estimates, up to 40% of private keys are affected.
At the moment, this problem has been solved, no new targets will be decrypted, there have been no bugs in the locker itself, and there never will be.

We are well aware of the consequences of this situation for the reputation of our product, this fact can undermine your trust in us, so we are ready to answer for this to you with our time and finances:
- All users of our product will be provided with a 100% rate for 3 weeks, regardless of whether or not you have targets that could potentially use the decryptor.
- All clients whose targets could potentially use the decryptor will be compensated from our deposit (currently around $ ~600k).

We very much hope that this situation will not undermine your trust in us, as we believe that trust is the foundation of our business. We are always ready to answer for any problems on our part and will never hide it.

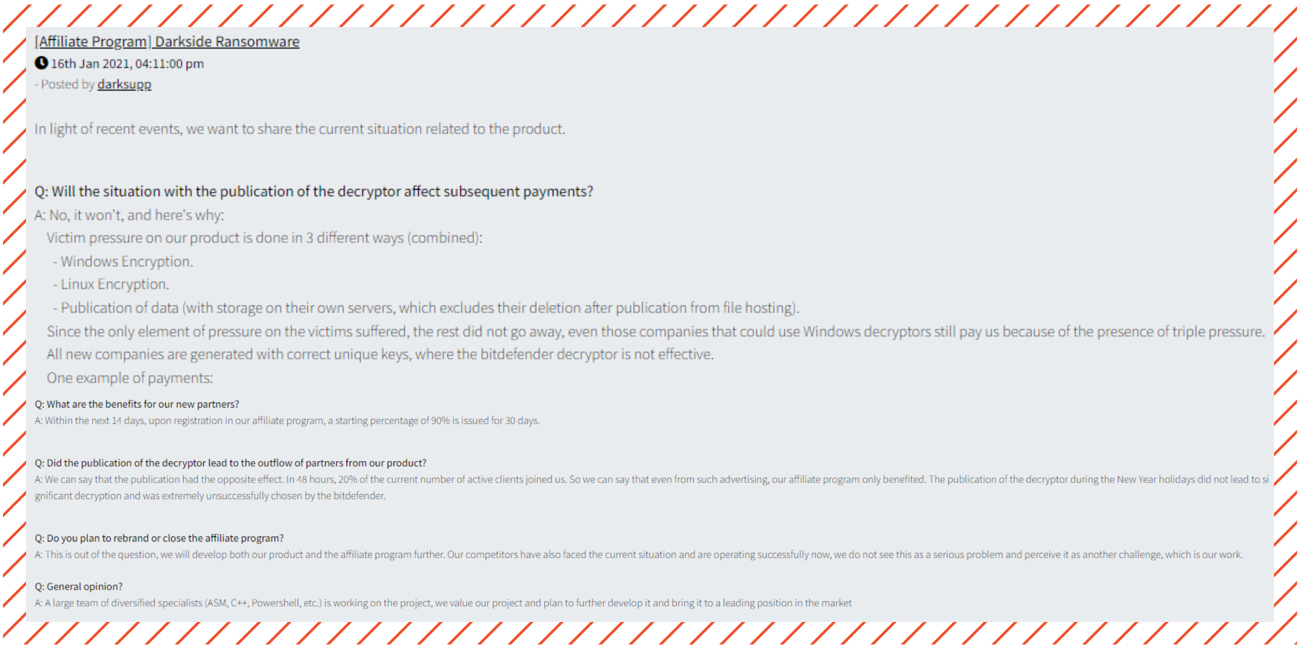
Special thanks to BitDefender for pointing out our shortcomings. This will make us even better. Now you will never decipher us ;)

Best regards, DarkSide team.

FIGURE 5: DARKSUPP SHARES AN UPDATE WITH AFFILIATES AS BITDEFENDER RELEASES A UTILITY THAT CAN DECRYPT SOME OF ITS WINDOWS LOCKERS.

Four days later, darksupp provided a Q&A on the product updates to answer its affiliates' questions **(Figure 6)**:

This communication is not only more professional than other RaaS groups, it also rivals many enterprises' customer service support.



[Affiliate Program] Darkside Ransomware
16th Jan 2021, 04:11:00 pm
- Posted by darksupp

In light of recent events, we want to share the current situation related to the product.

Q: Will the situation with the publication of the decryptor affect subsequent payments?
A: No, it won't, and here's why:
Victim pressure on our product is done in 3 different ways (combined):
- Windows Encryption.
- Linux Encryption.
- Publication of data (with storage on their own servers, which excludes their deletion after publication from file hosting).
Since the only element of pressure on the victims suffered, the rest did not go away, even those companies that could use Windows decryptors still pay us because of the presence of triple pressure.
All new companies are generated with correct unique keys, where the bitdefender decryptor is not effective.
One example of payments:

Q: What are the benefits for our new partners?
A: Within the next 14 days, upon registration in our affiliate program, a starting percentage of 90% is issued for 30 days.

Q: Did the publication of the decryptor lead to the outflow of partners from our product?
A: We can say that the publication had the opposite effect. In 48 hours, 20% of the current number of active clients joined us. So we can say that even from such advertising, our affiliate program only benefited. The publication of the decryptor during the New Year holidays did not lead to significant decryption and was extremely unsuccessfully chosen by the bitdefender.

Q: Do you plan to rebrand or close the affiliate program?
A: This is out of the question, we will develop both our product and the affiliate program further. Our competitors have also faced the current situation and are operating successfully now, we do not see this as a serious problem and perceive it as another challenge, which is our work.

Q: General opinion?
A: A large team of diversified specialists (ASM, C++, Powershell, etc.) is working on the project, we value our project and plan to further develop it and bring it to a leading position in the market

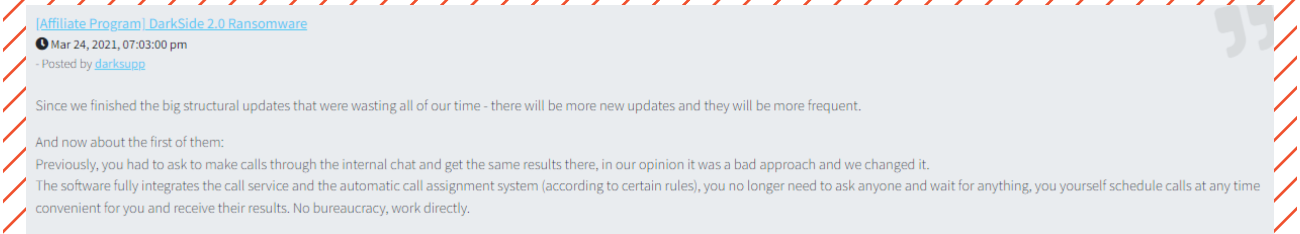
FIGURE 6: A DARKSIDE Q&A TO RESPOND TO CUSTOMER QUESTIONS AND CONCERNS.

ACTIVITY IN THE RUN-UP TO COLONIAL PIPELINE ATTACK

Insights into DarkSide's affiliate communications also show warning signs of increased activity in the months leading up to the Colonial Pipeline attack.

In January 2021, darksupp boasted on hacking forums of having an increased number of partners joining its RaaS affiliate programme. Then, in March 2021 - approximately one month before the initial compromise of Colonial Pipeline - it announced a change to its affiliate program on the forum Exploit, to remove "bureaucracy" by allowing its affiliates to "make calls" without asking the ransomware operators **(Figure 7)**.

> **INSIGHTS INTO DARKSIDE'S AFFILIATE COMMUNICATIONS ALSO SHOW WARNING SIGNS OF INCREASED ACTIVITY IN THE MONTHS LEADING UP TO THE COLONIAL PIPELINE ATTACK.**



[Affiliate Program] DarkSide 2.0 Ransomware

Mar 24, 2021, 07:03:00 pm

- Posted by darksupp

Since we finished the big structural updates that were wasting all of our time - there will be more new updates and they will be more frequent.

And now about the first of them:
Previously, you had to ask to make calls through the internal chat and get the same results there, in our opinion it was a bad approach and we changed it.
The software fully integrates the call service and the automatic call assignment system (according to certain rules), you no longer need to ask anyone and wait for anything, you yourself schedule calls at any time convenient for you and receive their results. No bureaucracy, work directly.

FIGURE 7: DARKSUPP ANNOUNCES A STRUCTURAL UPDATE TO THE AFFILIATE PROGRAM TO REMOVE BUREAUCRACY.

While we don't know the exact meaning of "calls" in this context, it seems implied that this change would allow affiliates more autonomy in their operations. If monitored, this could have signaled the potential for Darkside's affiliates to begin to take bigger risks and select larger targets.

ACTIONING DARK WEB THREAT INTELLIGENCE

The intelligence we can gather on these two groups from the dark web - and what this uncovers about differences between the two - is more than just a point of interest. There are clear instances where the availability of this intelligence at the time could have been used to inform an organization's cyber readiness for attacks.

For example, organizations operating in telecoms, software, gaming, call center, and the server hosting industries should have been on high alert for insider threat as soon as LAPSUS$ put out its call for recruits within these sectors. Likewise, "big game targets" should have shored up their ransomware preparedness and incident response procedures as DarkSide increased its affiliate numbers while simultaneously relaxing its rules for them.

During the operation of both groups, organizations should have investigated the access to company credentials that was already available on the dark web and in pastebins (T1589: Gather Victim Identity Information)[6], as this was the access point in a number of their attacks.

Of course, these examples are retrospective. In order for this intelligence to be most effective, monitoring has to be live and continuous. However, even months and years on, this information holds value because - while both LAPSUS$ and DarkSide have ceased in those monikers - our intelligence shows their membership are very likely carrying on under new aliases. Some LAPSUS$ threat actors are now thought to be operating under the names IMMORTAL$ and NWGEN, while it has been claimed by members themselves that DarkSide first morphed into BlackMatter gang, before moving on to develop the BlackCat/Alphv RaaS operation.

> “
> OUR INTELLIGENCE SHOWS THEIR MEMBERSHIP ARE VERY LIKELY CARRYING ON UNDER NEW ALIASES. SOME LAPSUS$ THREAT ACTORS ARE NOW THOUGHT TO BE OPERATING UNDER THE NAMES IMMORTAL$ AND NWGEN, WHILE IT HAS BEEN CLAIMED BY MEMBERS THEMSELVES THAT DARKSIDE FIRST MORPHED INTO BLACKMATTER GANG, BEFORE MOVING ON TO DEVELOP THE BLACKCAT/ALPHV RAAS OPERATION.

DARK WEB INTELLIGENCE FOR THE SUPPLY CHAIN

Adversarial intelligence is key for organizations looking to gain the upper hand on their attackers while they are in the Reconnaissance and Resource Development phases.

These two case studies of LAPSUS$ and DarkSide - two notable threat clusters from the past few years - demonstrate what we can learn about the TTPs used by each group from dark web intelligence.

As the contrast between the two groups shows, while the impact on the business might be the same, there are substantial differences between how threat groups operate. Therefore, treating all threat actors as a like-for-like threat is a mistake, and dark intelligence is one way organizations can create a more reliable picture of the adversary.

CASE ONE: M.E.DOC

INCIDENT OVERVIEW

In 2017 the NotPetya ransomware variant was distributed through a malicious update in the accounting software M.E.Doc by the Russian-backed hacking group Sandworm. Maersk was one of the highest-profile victims and worst affected.

The Danish shipping company was only saved from complete data loss by one of its Active Directory backups being offline in its powered-down office in Lagos.

IMPACT

Maersk reported[7] that:

4,000 Servers

45,000 PCs

2,500 Applications

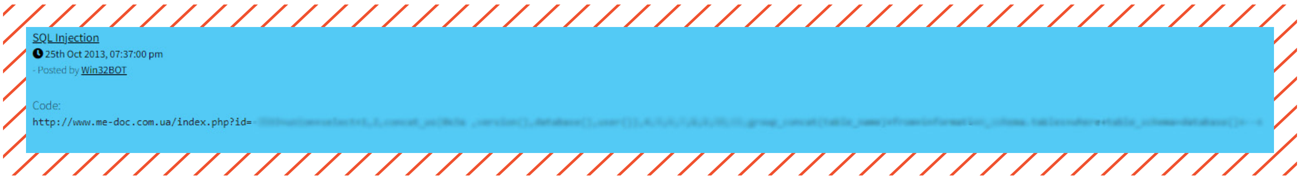
were impacted, with an estimated cost of:

$300M

To the business.

DARK WEB WARNING SIGNS

1. Mentions of vulnerabilities in the M.E.Doc website can be identified on the dark web as early as 2013 - four years prior to the incident (Figure 8).



SQL Injection
25th Oct 2013, 07:37:00 pm
- Posted by Win32BOT

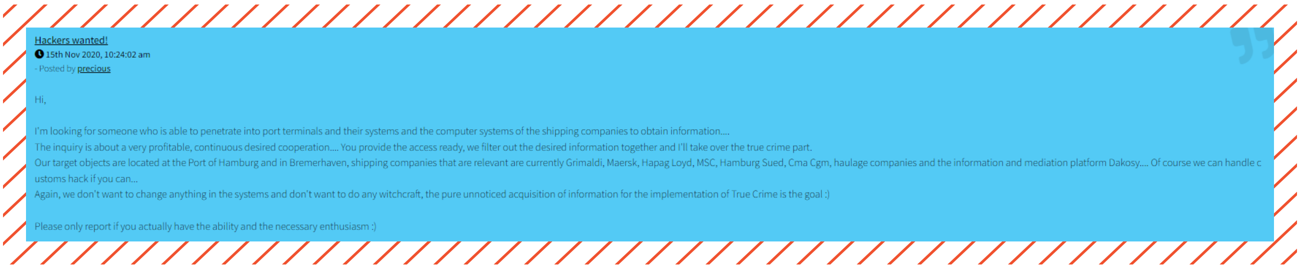
Code:

```
http://www.me-doc.com.ua/index.php?id=[redacted]
```

FIGURE 8: WIN32BOT POSTS A SQL INJECTION FOR M.E.DOC IN 2013.

2. Spam templates specifically tailored to Maersk can also be found from the same time, demonstrating that the company was on the radar of cybercriminals.

3. There were multiple conversations on forums among threat actors that were inspired by the original Petya ransomware and were seeking malware that could achieve similar results by overwriting the Master Boot Record of the infected system (Figure 9).



Hackers wanted!
15th Nov 2020, 10:24:02 am
- Posted by precious

Hi,

I'm looking for someone who is able to penetrate into port terminals and their systems and the computer systems of the shipping companies to obtain information....
The inquiry is about a very profitable, continuous desired cooperation.... You provide the access ready, we filter out the desired information together and I'll take over the true crime part.
Our target objects are located at the Port of Hamburg and in Bremerhaven, shipping companies that are relevant are currently Grimaldi, Maersk, Hapag Loyd, MSC, Hamburg Sued, Cma Cgm, haulage companies and the information and mediation platform Dakosy.... Of course we can handle c ustoms hack if you can...
Again, we don't want to change anything in the systems and don't want to do any witchcraft, the pure unnoticed acquisition of information for the implementation of True Crime is the goal :)

Please only report if you actually have the ability and the necessary enthusiasm :)

FIGURE 9: ANALYSIS OF DARK WEB ACTIVITY SUGGESTS THAT, IN THE AFTERMATH OF THE 2017 ATTACK, MAERSK CONTINUES TO BE AN ACTIVE TARGET. FOR EXAMPLE, IN 2020 THE FIRM WAS NAMED BY A THREAT ACTOR SEEKING INITIAL ACCESS TO THE COMPUTER SYSTEMS OF PORT TERMINALS AND VARIOUS SHIPPING COMPANIES WITH INTENT TO STEAL INFORMATION.

CASE TWO: KRONOS

INCIDENT OVERVIEW

In 2021 Ultimate Kronos Group was the victim of a ransomware attack on its private cloud platform. This attack impacted the enterprises that used the payroll and workforce management company, including Whole Foods, GameStop, Honda, and many large US healthcare groups such as Ascension.

IMPACT

It has been estimated[8] that some

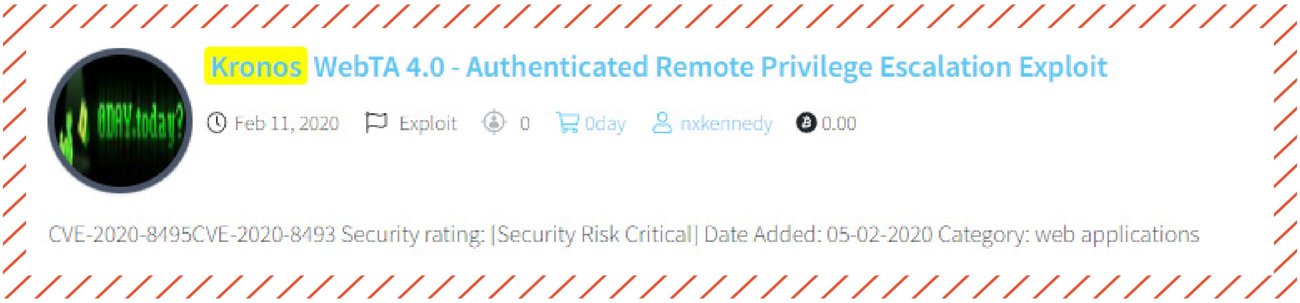
8,000,000

people were affected by this attack against one supply chain company. Workers at Tesla, PepsiCo. and from the New York transit system filed lawsuits against the Ultimate Kronos Group.

DARK WEB WARNING SIGNS

1 Records on the dark web show that Kronos was on threat actors' radars as far back as the time of the Maersk compromise.

2 In 2020, a full year before the attack itself, an apparent Kronos web application exploit that enabled remote privilege escalation was for sale on a dark web market **(Figure 10)**.



Kronos WebTA 4.0 - Authenticated Remote Privilege Escalation Exploit

Feb 11, 2020 Exploit 0 0day nxkennedy 0.00

CVE-2020-8495CVE-2020-8493 Security rating: |Security Risk Critical| Date Added: 05-02-2020 Category: web applications

FIGURE 10: KRONOS EXPLOIT LISTED FOR SALE IN FEBRUARY 2020.

3 By the end of 2021, a threat actor was posting adverts for exfiltrated Kronos records for sale.

CASE THREE: KASEYA

INCIDENT OVERVIEW

In July 2021 cybercriminals used a zero day vulnerability in Kaseya's Virtual Systems Administrator (VSA) software to bypass authentication, run arbitrary command execution, and deploy ransomware to endpoints. This attack was made worse by the fact that Kaseya is a supplier to managed service providers (MSPs), who each in turn had dozens of customers who were affected.

IMPACT

In total, it is estimated[9] that more than

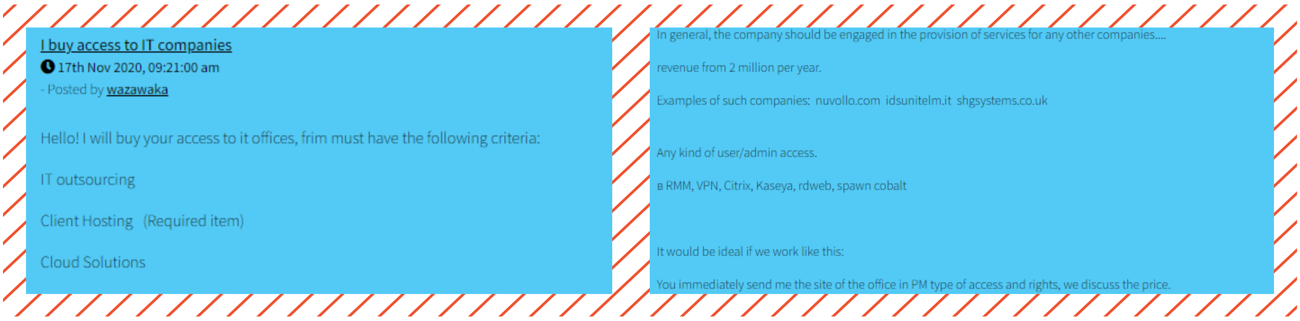
1000

COMPANIES

had their endpoints encrypted as a result of the Kaseya vulnerability.

DARK WEB WARNING SIGNS

1. Threat actors were discussing the exploitation of Kaseya in dark web forums two years before the attack.
2. Those discussions suggested an old vulnerability already existed in a Kaseya plugin and was being actively exploited to deploy Gandcrab ransomware downstream to customers.
3. In 2020 there were requests to buy access to IT outsourcing companies, with Kaseya being explicitly named as a route of entry (Figure 11).



I buy access to IT companies

🕓 17th Nov 2020, 09:21:00 am

- Posted by wazawaka

Hello! I will buy your access to it offices, frim must have the following criteria:

IT outsourcing

Client Hosting (Required item)

Cloud Solutions

In general, the company should be engaged in the provision of services for any other companies....

revenue from 2 million per year.

Examples of such companies: nuvollo.com idsunitelm.it shgsystems.co.uk

Any kind of user/admin access.

в RMM, VPN, Citrix, Kaseya, rdweb, spawn cobalt

It would be ideal if we work like this:

You immediately send me the site of the office in PM type of access and rights, we discuss the price.

FIGURE 11: WAZAWAKA REQUESTS ACCESS TO IT COMPANIES, SUGGESTING KASEYA AS AN ENTRY POINT.

4. Searchlight has identified 21 different Kaseya account credentials that were up for sale in 2020.

EARLY WARNING SIGNS IN THE DARK WEB

In each of these instances, dark web intelligence gives us more than just an indication that supply chain companies are being targeted by threat actors (most probably are). It also tells us the specific vulnerabilities that cybercriminals were trying to exploit with each supply chain company and, for Kronos, when the criminals had succeeded in exfiltrating data.

> **MONITORING THE DARK WEB FOR THEIR SUPPLIERS IS ONE OF THE BEST WAYS ORGANIZATIONS CAN GET A TRUE SENSE OF THEIR SUPPLY CHAIN RISK.**

This is just the tip of the iceberg of what can be gleaned from dark web supply chain intelligence. Monitoring the dark web for their suppliers is one of the best ways organizations can get a true sense of their supply chain risk. Not relying on what their third parties have disclosed or are claiming, but with specific intelligence that enables them to take action and mitigate the risk of attack via a third party.

MAPPING DARK WEB INTELLIGENCE TO THE MITRE ATT&CK FRAMEWORK

Each of these cases demonstrates how dark web intelligence shines a light on criminals while they are in their pre-attack phase. In many cases, this intelligence can be directly mapped onto the PRE Matrix techniques of the MITRE ATT&CK framework.
As just three examples:

> DARK WEB INTELLIGENCE CAN BE DIRECTLY MAPPED ONTO THE PRE MATRIX TECHNIQUES OF THE MITRE ATT&CK FRAMEWORK.

MITRE ATT&CK TECHNIQUE	TECHNIQUE SUMMARY	ROLE OF DARK WEB INTELLIGENCE
Active Scanning (T1595)[10]	Adversaries execute active reconnaissance scans to gather information that can be used during targeting, probing the victim's infrastructure via network traffic.	Monitoring incoming network traffic from the dark web to your organization provides a clear indicator that cyber criminals are conducting reconnaissance against your network, allowing you to assess when they are going to attack and what their path of entry may be.
Gather Victim Identity Information (T1589)[11]	Adversaries gather information about the victim's identity that can be used during targeting. This information may include personal data (employee names, email addresses, etc.) as well as sensitive details such as credentials.	Dark web monitoring can identify usernames, emails, and passwords associated with a company that have been leaked or are being sold on the dark web, in markets or being discussed on forums. Having oversight of this information enables organizations to update passwords and enforce access controls.
Search Closed Sources (T1597)[12]	Adversaries search and gather information about victims from closed sources that can be used during targeting. Information about victims may be available for purchase from reputable private sources and databases, such as paid subscriptions to feeds of technical/threat intelligence data.	Monitoring dark web markets, forums, paste sites and leaks, will allow an organization to identify leaked attributes associated with the company, as well as conversations regarding the organization. Identification of dark web chatter allows security teams to take additional precautions to protect the network from a potential attack.

UNLOCK PRE-ATTACK INTELLIGENCE FROM THE DARK WEB

WHETHER YOU ARE MAPPING YOUR PRE-ATTACK INTELLIGENCE TO THE MITRE ATT&CK FRAMEWORK OR NOT, SEARCHLIGHT SECURITY CAN HELP YOU INCREASE YOUR VISIBILITY INTO EARLY WARNING SIGNS OF ATTACK ON THE DARK WEB:

UNDERSTAND DARK WEB RISK EXPOSURE

Get an instant health report of your organization's external threat exposure on the dark web and make decisions from Searchlight's intuitive, easy to use interface.

GAIN PRE-ATTACK INTELLIGENCE AND INVESTIGATION CAPABILITIES

Enhance your threat intelligence and threat monitoring capabilities with an unmatched window into activity on dark web forums, marketplaces and conversations, without any risk to your analysts.

IDENTIFY THE EARLY WARNING SIGNS OF ATTACK

Receive automatic alerts for indicators of malicious activity against your business, such as leaked credentials, IP addresses, open ports, and compromised devices.

MONITOR DARK WEB TRAFFIC

Get visibility of both inbound and outbound dark web traffic from your network, where it is coming from and where it is going, so you can identify the signs of an external attack or insider threat.

MITIGATE THIRD PARTY RISK

Remotely monitor the exposure of your third party suppliers and partners on the dark web without the need for an agent on their systems, to prevent supply chain attacks and prove compliance.

INFORM INCIDENT INVESTIGATION AND RESPONSE

Forensically examine the chain of events in the dark web that led to an attack to inform incident mitigation and response.

VISIT **WWW.SLCYBER.IO** TO FIND OUT MORE OR BOOK A DEMO NOW.

REFERENCES

PAGE 5

1. https://attack.mitre.org/matrices/enterprise/
2. https://attack.mitre.org/tactics/TA0043/
3. https://attack.mitre.org/tactics/TA0043/
4. https://attack.mitre.org/matrices/enterprise/pre/

PAGE 10

5. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password#xj4y7vzkg

PAGE 13

6. https://attack.mitre.org/techniques/T1589/

PAGE 15

7. https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/

PAGE 16

8. https://threatpost.com/kronos-dragging-itself-back-ransomware-hell/178213/

PAGE 17

9. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

PAGE 19

10. https://attack.mitre.org/techniques/T1595
11. https://attack.mitre.org/techniques/T1589
12. https://attack.mitre.org/techniques/T1597

SEARCHLIGHT.
CYBER

VISIT **WWW.SLCYBER.IO** TO FIND
OUT MORE OR BOOK A DEMO NOW.

UK HEADQUARTERS
Suite 63, Pure Offices,
1 Port Way, Port Solent,
Portsmouth PO6 4TY
United Kingdom

US HEADQUARTERS
900 16th Street NW,
Suite 450, Washington,
DC 20006
United States