A Real-World Look at How Cybercriminals Use the Dark Web to Target Banking Organizations

by Ariel Ainhoren / June 5, 2018

So, it's time to go to the bank again. As you wait in line, you look around and think about the security measures around you: big vaults, security cameras, and even bulletproof glass at the counter. On the surface, everything looks secure, but if a trained thief stood there instead of you, they would see all the faults in the bank's security, like dead spots in the security camera coverage, predictable shift changes, corruptible personnel, or old, penetrable locks.

The same goes for the online world. When you log in to your bank's website, transfer money through 3rd party apps, or use your Google or Apple pay, hackers will always try to interfere and steal the personal data that flows between financial systems. They will shadow and mimic the ways people use technology and try to exploit them to their advantage.

In this blog, we will show you some of the holes that hackers see in a bank's cybersecurity systems by giving you a glimpse into the Deep and Dark Web threat profile of an IntSights medium-sized bank client.

Bank Dark Web Profile

Hackers follow the money, so banks and their customers are always a target for hackers. An attacker's eye will always search for the shortest way to make the biggest profit. As a cybersecurity professional, it's important to understand how hackers view your organization so that you can identify weaknesses and take proactive measures to protect your company and your customers.

Here are our findings for one of our banking clients (which for obvious reasons, we will keep anonymous) over the course of the last year:

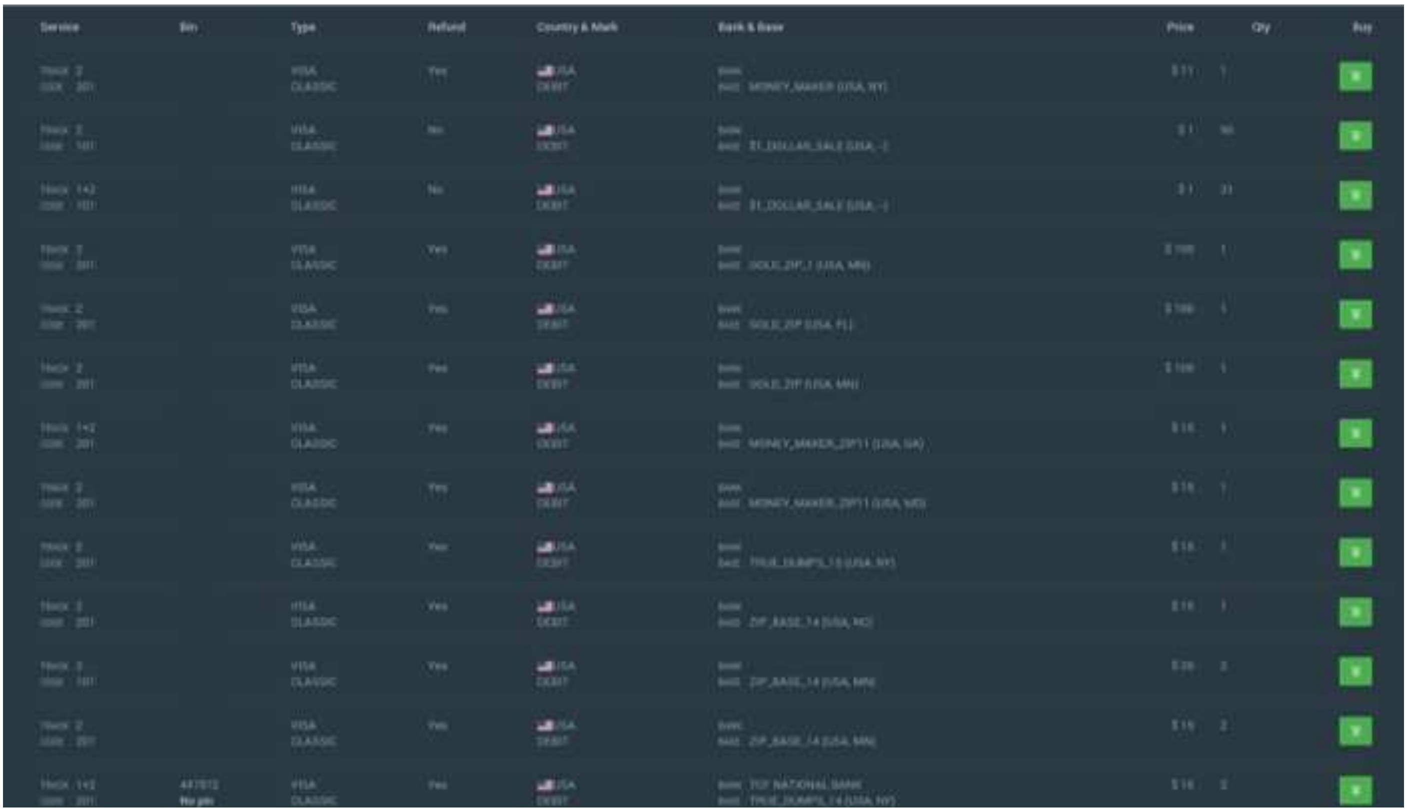
1. Credit Cards

Hackers love credit card information. They obtain it through both virtual and physical vulnerabilities, like point of sale malware, exposed databases, phishing and spear phishing attacks, ATM skimmers, and even corrupted individuals (aka "insiders"). Some of the information is for the hacker's own use, but most of it ends up in black markets that offer it for sale – per card, or in bulk purchases. High-end Platinum cards cost more, while small debt cards can cost a single dollar. This information is often used later in fraud schemes or to acquire different goods in the real world.

Our Real-World Findings

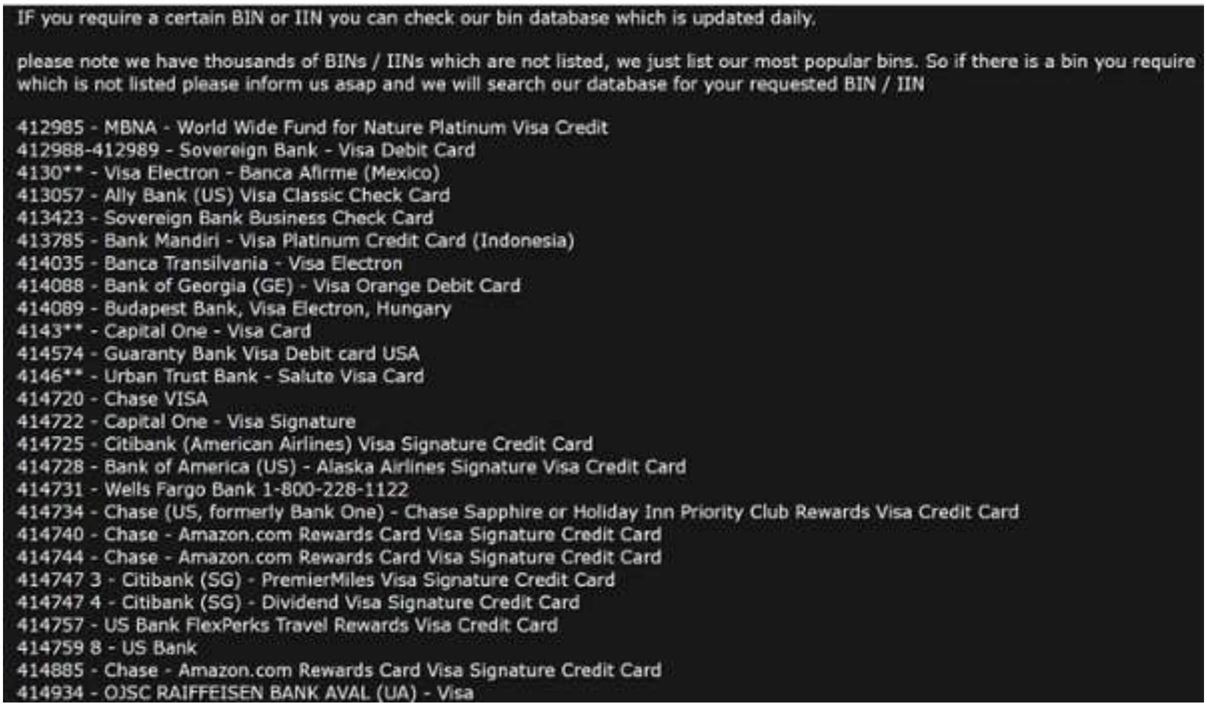
Over the last year, we identified 76 alerts of credit card leakages for this bank; with each alert containing hundreds of credit card numbers (Figure 1).

Some Black Market vendors have favorite bank lists because of the different security measures each bank takes, or because of the sheer size of the bank. Big banks have relatively strong security measures for their online systems, but their size is a disadvantage, as they can't protect every branch and office with the same measures. Therefore, they are susceptible to fraud and impersonation. Small banks sometimes lack sufficient online security measures, but their size and personal relations with their customers make them less susceptible to fraud.



Service	Bin	Type	Refund	Country & Mark	Bank & Base	Price	Qty	Buy
Track 2 Code 201		VISA CLASSIC	Yes	USA DEBIT	bank base MONEY_MAKER (USA, NY)	$ 11	1	
Track 2 Code 101		VISA CLASSIC	No	USA DEBIT	bank base $1_DOLLAR_SALE (USA, -)	$ 1	50	
Track 1+2 Code 101		VISA CLASSIC	No	USA DEBIT	bank base $1_DOLLAR_SALE (USA, -)	$ 1	21	
Track 2 Code 201		VISA CLASSIC	Yes	USA DEBIT	bank base GOLD_ZIP_1 (USA, MN)	$ 100	1	
Track 2 Code 201		VISA CLASSIC	Yes	USA DEBIT	bank base GOLD_ZIP (USA, FL)	$ 100	1	
Track 2 Code 201		VISA CLASSIC	Yes	USA DEBIT	bank base GOLD_ZIP (USA, MN)	$ 100	1	
Track 1+2 Code 201		VISA CLASSIC	Yes	USA DEBIT	bank base MONEY_MAKER_ZIP11 (USA, GA)	$ 16	1	
Track 2 Code 201		VISA CLASSIC	Yes	USA DEBIT	bank base MONEY_MAKER_ZIP11 (USA, MD)	$ 15	1	
Track 2 Code 201		VISA CLASSIC	Yes	USA DEBIT	bank base TRUE_DUMPS_15 (USA, NY)	$ 16	1	
Track 2 Code 201		VISA CLASSIC	Yes	USA DEBIT	bank base ZIP_BASE_14 (USA, NC)	$ 16	1	
Track 2 Code 101		VISA CLASSIC	Yes	USA DEBIT	bank base ZIP_BASE_14 (USA, MN)	$ 26	2	
Track 2 Code 201		VISA CLASSIC	Yes	USA DEBIT	bank base ZIP_BASE_14 (USA, MN)	$ 15	2	
Track 1+2 Code 201	447872 No pin	VISA CLASSIC	Yes	USA DEBIT	bank TCF NATIONAL BANK base TRUE_DUMPS_14 (USA, NY)	$ 16	2	

Figure 1: Credit Cards for Sale



IF you require a certain BIN or IIN you can check our bin database which is updated daily.

please note we have thousands of BINs / IINs which are not listed, we just list our most popular bins. So if there is a bin you require which is not listed please inform us asap and we will search our database for your requested BIN / IIN

412985 - MBNA - World Wide Fund for Nature Platinum Visa Credit
412988-412989 - Sovereign Bank - Visa Debit Card
4130** - Visa Electron - Banca Afirme (Mexico)
413057 - Ally Bank (US) Visa Classic Check Card
413423 - Sovereign Bank Business Check Card
413785 - Bank Mandiri - Visa Platinum Credit Card (Indonesia)
414035 - Banca Transilvania - Visa Electron
414088 - Bank of Georgia (GE) - Visa Orange Debit Card
414089 - Budapest Bank, Visa Electron, Hungary
4143** - Capital One - Visa Card
414574 - Guaranty Bank Visa Debit card USA
4146** - Urban Trust Bank - Salute Visa Card
414720 - Chase VISA
414722 - Capital One - Visa Signature
414725 - Citibank (American Airlines) Visa Signature Credit Card
414728 - Bank of America (US) - Alaska Airlines Signature Visa Credit Card
414731 - Wells Fargo Bank 1-800-228-1122
414734 - Chase (US, formerly Bank One) - Chase Sapphire or Holiday Inn Priority Club Rewards Visa Credit Card
414740 - Chase - Amazon.com Rewards Card Visa Signature Credit Card
414744 - Chase - Amazon.com Rewards Card Visa Signature Credit Card
414747 3 - Citibank (SG) - PremierMiles Visa Signature Credit Card
414747 4 - Citibank (SG) - Dividend Visa Signature Credit Card
414757 - US Bank FlexPerks Travel Rewards Visa Credit Card
414759 8 - US Bank
414885 - Chase - Amazon.com Rewards Card Visa Signature Credit Card
414934 - OJSC RAIFFEISEN BANK AVAL (UA) - Visa

Figure 2: Dark Web Vendor's Favorite Bank List

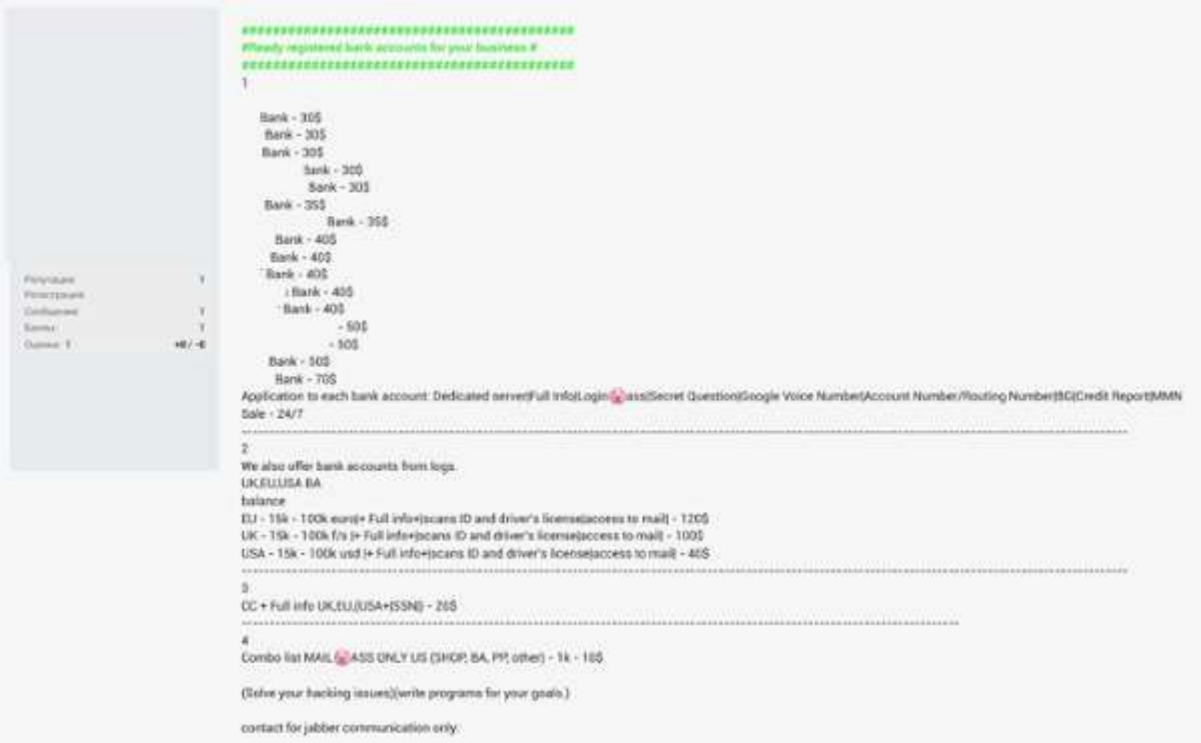
Click to See Expanded Full List

2. Bank Account Details

Apart from credit cards, hackers like to steal and trade bank account information. Account information contains the full data of the account, including full name, address, account number, account balance, login credentials, security questions, credit report, personal email used for login, etc. (see Figure 3). Other types of bank details are bank document templates to be used in fraud scenarios (see Figure 4). The full account details can be used in a multitude of different fraud scenarios, like tax fraud, credit card issuance, insurance claims, loan taking, and more.

Real-World Findings

We found over 45 instances of leaked bank account details, each instance containing hundreds of different leaked accounts. These bank account details can be used for fraudulent activities, like draining the account or using it for online gambling.



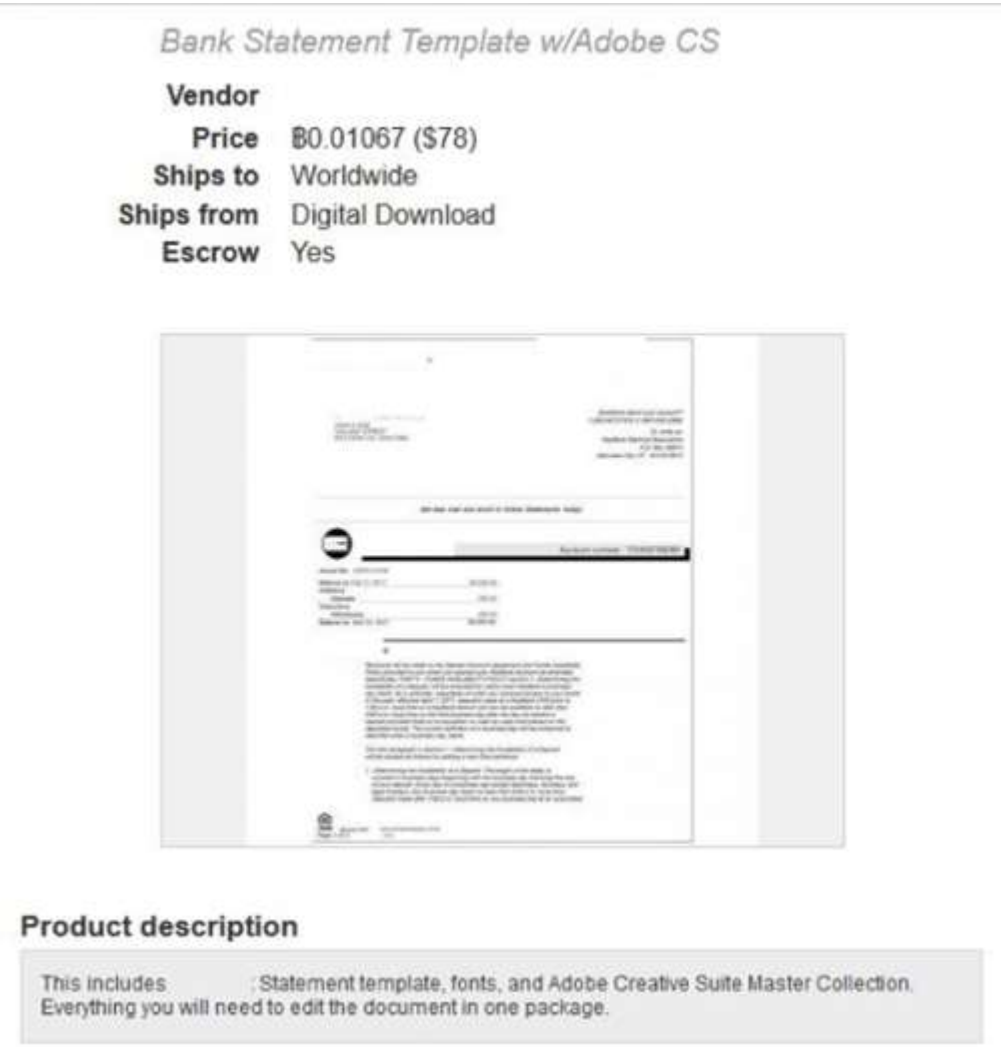
```
############################################
#Ready registered bank accounts for your business #
############################################
1

   Bank - 30$
    Bank - 30$
   Bank - 30$
            Bank - 30$
             Bank - 30$
    Bank - 35$
                 Bank - 35$
      Bank - 40$
     Bank - 40$
    Bank - 40$
         : Bank - 40$
        Bank - 40$
                   - 50$
                  - 50$
     Bank - 50$
      Bank - 70$
Application to each bank account: Dedicated server|Full info|Login😡ass|Secret Question|Google Voice Number|Account Number/Routing Number|BG|Credit Report|MMN
Sale - 24/7
-----------------------------------------------------------------------------------------------------------------------
2
We also offer bank accounts from logs.
UK,EU,USA BA
balance
EU - 15k - 100k euro|+ Full info+|scans ID and driver's license|access to mail| - 120$
UK - 15k - 100k f/s |+ Full info+|scans ID and driver's license|access to mail| - 100$
USA - 15k - 100k usd |+ Full info+|scans ID and driver's license|access to mail| - 40$
-----------------------------------------------------------------------------------------------------------------------
3
CC + Full info UK,EU,(USA+(SSN)) - 26$
----------------------------------------------------------------------------------------------
4
Combo list MAIL😡ASS ONLY US (SHOP, BA, PP, other) - 1k - 10$

(Solve your hacking issues)(write programs for your goals.)

contact for jabber communication only.
```

Figure 3: Bank Account Details Offered for Sale



Bank Statement Template w/Adobe CS

Vendor	
Price	฿0.01067 ($78)
Ships to	Worldwide
Ships from	Digital Download
Escrow	Yes

Product description

This includes :Statement template, fonts, and Adobe Creative Suite Master Collection. Everything you will need to edit the document in one package.

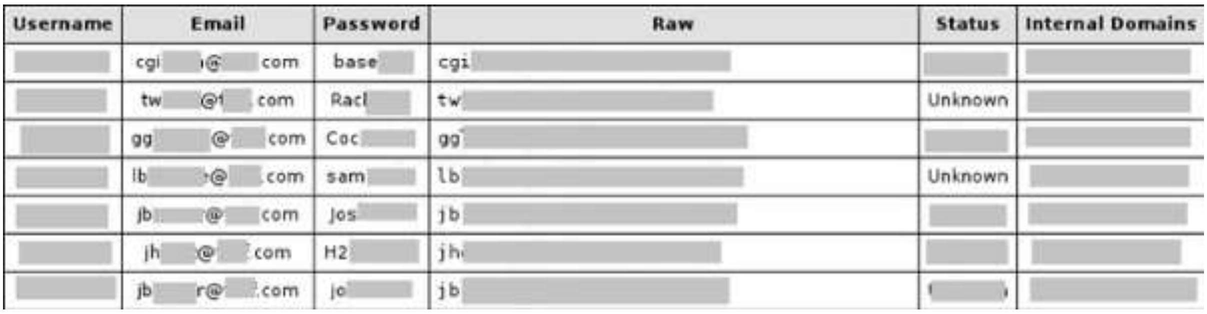
Figure 4: Bank Document Templated Offered for Sale

3. Leaked Credentials of Bank Employees

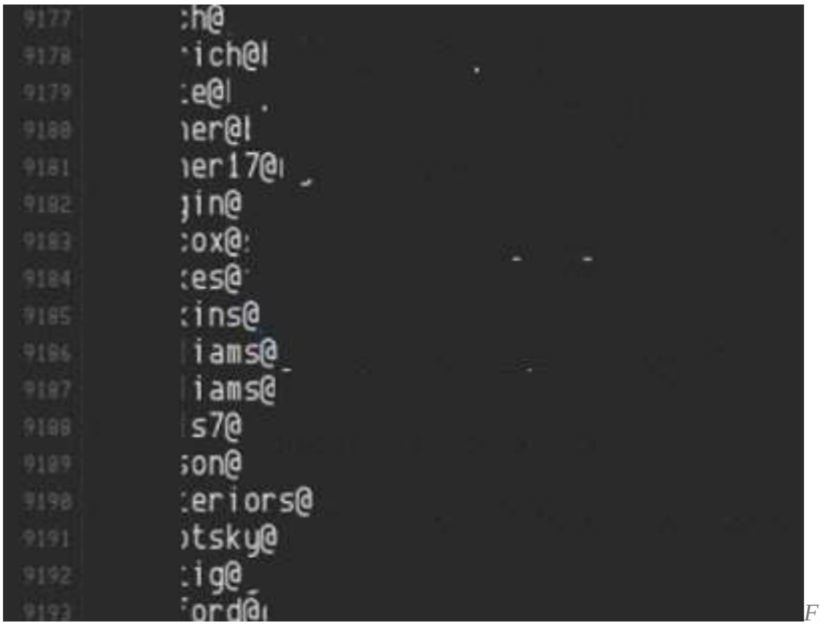
Another great target for hackers are bank employees. Leaked employee credentials give hackers access to bank systems, which helps them access additional bank account data, or use that employee account as a staging ground for further phishing attacks on other bank employees. High-quality credentials, such as those of the IT staff or bank management, can sell for a steep price, and can generate revenue in dozens of ways to defraud bank customers, employees, and affiliates.

Real-World Findings

We uncovered 40 sources containing hundreds of leaked bank employee credentials. The sources were versatile, ranging from leaked hacked databases, black markets, and insider information. Some of the data was gathered through multiple sources, matching company email and usernames with other leaked data of those employees, which used identical passwords for both personal and business accounts (Figures 5 & 6).



Username	Email	Password	Raw	Status	Internal Domains
[redacted]	cgi[redacted]@[redacted]com	base[redacted]	cgi[redacted]	[redacted]	[redacted]
[redacted]	tw[redacted]@[redacted] com	Racl[redacted]	tw[redacted]	Unknown	[redacted]
[redacted]	gg[redacted]@[redacted]com	Coc[redacted]	gg[redacted]	[redacted]	[redacted]
[redacted]	lb[redacted]@[redacted]com	sam[redacted]	lb[redacted]	Unknown	[redacted]
[redacted]	jb[redacted]@[redacted]com	Jos[redacted]	jb[redacted]	[redacted]	[redacted]
[redacted]	jh[redacted]@[redacted]com	H2[redacted]	jh[redacted]	[redacted]	[redacted]
[redacted]	jb[redacted]r@[redacted].com	jo[redacted]	jb[redacted]	[redacted]	[redacted]



```
:h@
:ich@l
:e@l
ıer@l
ıer17@ı
ȷin@
:ox@:
:es@
:ins@
 iams@
 iams@
 s7@
;on@
:eriors@
ɔtsky@
:ig@
:ord@ı
```

Figures 5 & 6: Leaked Bank Employee Credentials

Conclusion

Because banks and financial institutions deal with money so closely, malicious actors see them and their customers as an endless resource for scams and profit making. This blog looks at just one out of thousands of banks, and we only showed the tip of the iceberg. There are many other ways hackers exploit banks and their clients to make money. In our day-to-day work, we see conversations, guides, and even business proposals between hackers regarding different bank fraud strategies and scams to make money out of the information they obtain. New ways are invented daily to exploit weak links, vulnerabilities and unaware users. Knowing how hackers plan attacks and view your organization can help you prevent fraud before it happens.

5 Indicators of Attack You Can Uncover with Dark Web Monitoring

by Nathan Teplow / May 30, 2018

The Dark Web has received a lot of attention recently, and is often portrayed as a scary, mysterious place where cyber criminals steal identities and purchase illegal goods. While this is true, the Dark Web can actually be a great source of threat intelligence. Hackers and Advanced Persistent Threat (APT) groups often plan out their cyber attacks using the Dark Web, performing activities like reconnaissance, buying malware programs or sharing leaked credentials.

Monitoring this Dark Web activity can help you anticipate cyber attacks against your organization and identify gaps in coverage prior to them being exploited. So what should you be looking for exactly? Here are 5 indicators of attack that you should be monitoring for on the Dark Web.

#1: Corporate Reconnaissance

The first step of any cyber attack is reconnaissance, which is one of the primary uses of the Dark Web by cyber criminals. Hackers and APT groups try to collect as much information as possible to help in their attacks. For example, they will look for potential vulnerabilities, leaked employee credentials, software programs in use and details about the IT infrastructure.

To do this, cyber criminals will typically purchase information or recruit people with knowledge of the target company. Tracking these requests and interactions can help you identify certain users or groups targeting your organization and figure out how they might attack you. This enables you to identify weak spots in your security infrastructure and take proactive measures to defend against an attack.

#2: Phishing Targeting

Hackers typically coordinate their phishing attacks using the Dark Web before they are launched against a user. Attackers don't always engineer the entire phishing scheme. For example, they may recruit someone with web design experience to build a website that mimics a known or popular site. They may even purchase the actual ransomware program they plan to deploy using the phishing site.

The scary thing about phishing attacks is that nothing has to be breached or exploited for them to be carried out, so they can be difficult to monitor for. However, you still have an obligation to protect your employees and customers from phishing attacks that use your company's name or brand.

Monitoring the Dark Web for phishing attack coordination can help you identify and takedown phishing sites before they're ever used, protecting your employees, customers and brand reputation.

#3: Recruiting Company Insider

No matter how strong your cyber defenses are, a company insider can always bypass them and leak information. Cyber criminals know this is one of the best ways to access confidential information and frequently use the Dark Web to recruit company insiders. In addition, they may post or share lists of potential employees for recruitment, which can also be used to indicate a potential attack or leak.

Monitoring forums and list sharing on the Dark Web can help you identify when an adversary may try to recruit an insider from your organization.

#4: Buying or Selling Login Credentials

Buying and selling leaked credentials is a common practice across the Dark Web. Obviously, it's very easy for someone to access your sensitive information if they have active login credentials. Locking down leaked credentials is essential to keeping your data safe, and monitoring the Dark Web for purchases or requests for login credentials can help you identify data leaks and lock down accounts before they're exploited.

#5: Credit Card, Bank Account Logins & BINs for Sale

Another “good” that is frequently bought and sold using the Dark Web is financial information, like credit card numbers, bank account login credentials or Bank Identification Numbers (BINs). It’s important to monitor for any financial information being shared on the Dark Web to help protect your employees and customers against fraudulent charges.

Even if you are not a financial services company, it’s still important to monitor for any corporate bank accounts or credit cards that may be shared or targeted on the Dark Web.

Conclusion

The Dark Web is definitely a place for illegal activity, and it may not be a place you ever want to visit. However, monitoring these interactions, forums and marketplaces on the Dark Web can be a critical source of threat intelligence, enabling you to proactively protect your organization, rather than react to attacks. Dark Web monitoring allows you to be where your adversaries are and see your organization like an attacker would. Therefore, cybersecurity professionals must know about how the Dark Web is used and what to monitor for.

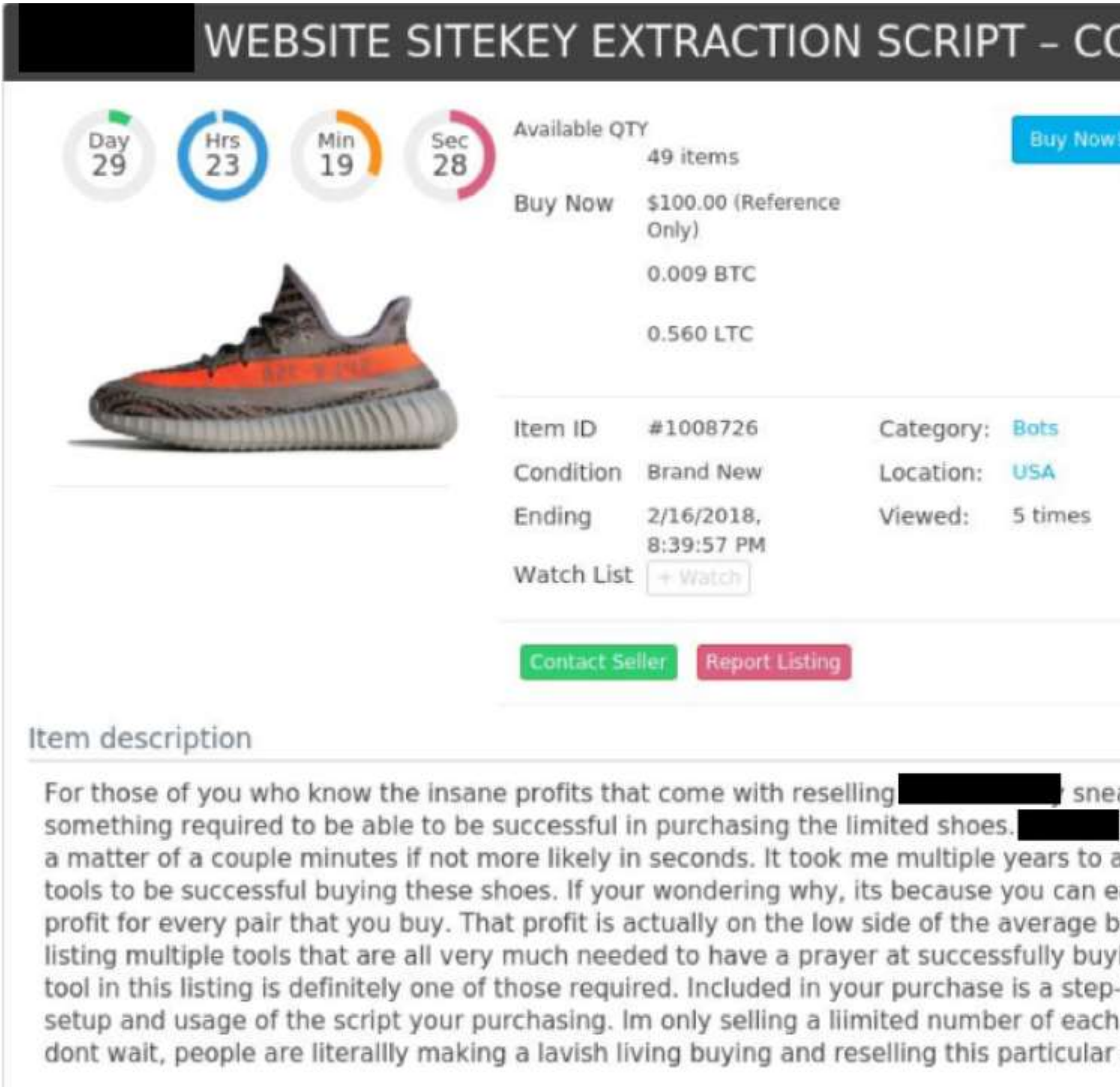
Want to learn more about the Dark Web and how it’s used by cyber criminals? Download our Dark Web 101 Guide today.

Dark Web 101: What Every Security Professional Needs to Know

Download: Dark Web 101

A Common Retailer Dark Web Profile: What We Found In Our Search

by Orin Mor / June 14, 2018



[redacted] WEBSITE SITEKEY EXTRACTION SCRIPT – CC

Available QTY	49 items		
Buy Now	$100.00 (Reference Only) 0.009 BTC 0.560 LTC		
Item ID	#1008726	Category:	Bots
Condition	Brand New	Location:	USA
Ending	2/16/2018, 8:39:57 PM	Viewed:	5 times
Watch List	+ Watch		

Item description

For those of you who know the insane profits that come with reselling [redacted] snea
something required to be able to be successful in purchasing the limited shoes. [redacted]
a matter of a couple minutes if not more likely in seconds. It took me multiple years to a
tools to be successful buying these shoes. If your wondering why, its because you can e
profit for every pair that you buy. That profit is actually on the low side of the average b
listing multiple tools that are all very much needed to have a prayer at successfully buy
tool in this listing is definitely one of those required. Included in your purchase is a step-
setup and usage of the script your purchasing. Im only selling a liimited number of each
dont wait, people are literallly making a lavish living buying and reselling this particular

The Dark Web has evolved over the past few years in many ways, but one of the biggest changes is the amount of information you can find via Dark Web forums and black markets. This increase in Dark Web data developed when hackers started focusing on new targets that weren't in the landscape before. As more industries move their businesses online, their digital attack surfaces have increased dramatically, which has given hackers new targets and scam opportunities. One of the new victims of this shift is the retail and the eCommerce sector.

For this blog, we will share examples of common retailer data found across the Dark Web and build a "Dark Web profile" for a typical retail company.

How Hackers Target Retail Companies

Imagine you run a successful eCommerce site. After a recent ad campaign, you see that every product you sell is sold out within seconds after you ran the ad. You go home to your family and celebrate your success, but little do you know that a hacker has targeted your site and bought your whole stock of products, making it unavailable to your typical customers.

These products are later being sold on dark web platforms by the hacker, who is making hundreds of dollars in profits from selling your product that is not in stock anymore (which they forced with their original purchase). It doesn't take long for your customers to become upset, and your site’s reputation begins to fall.

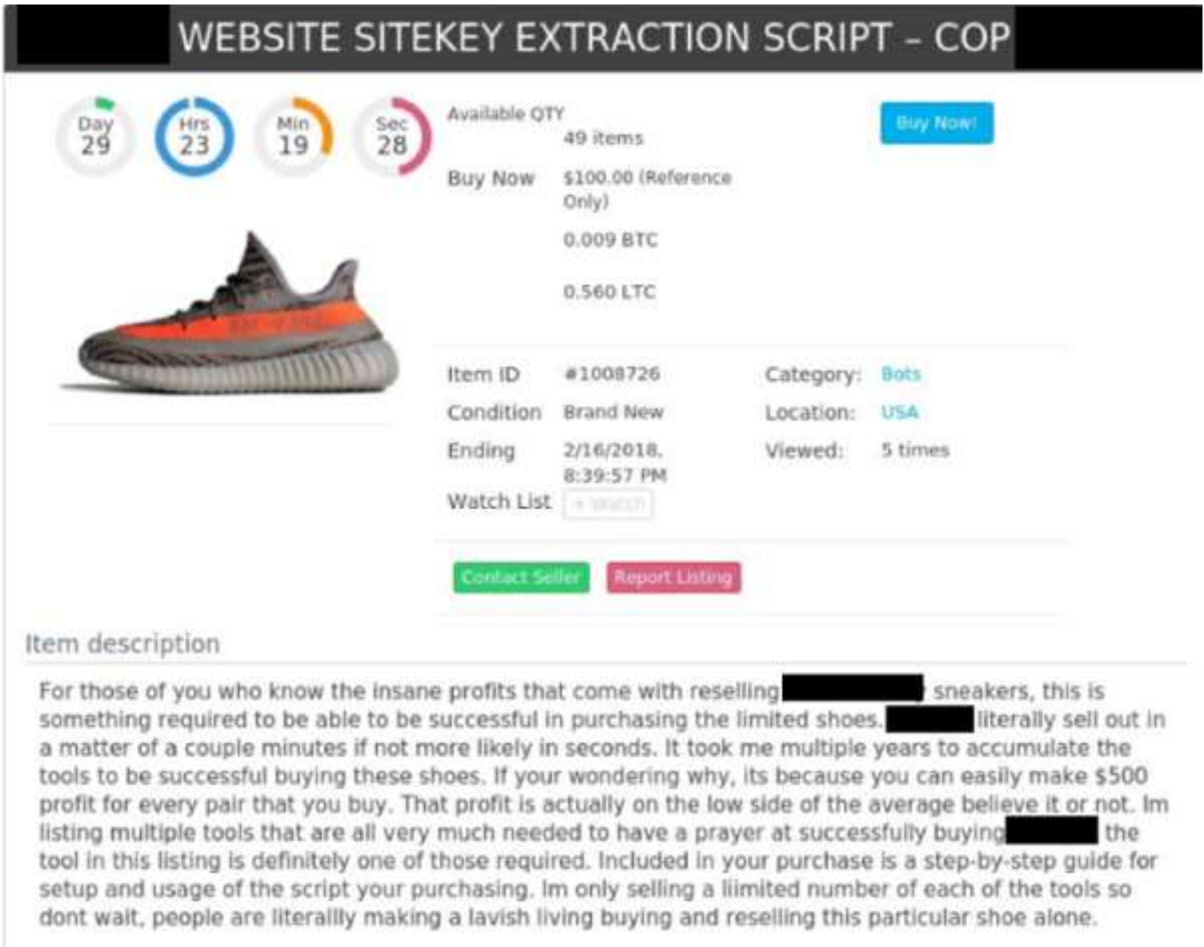
These cyber attacks against Retail and eCommerce shops can be incredibly damaging to both profits and reputation. Yet, many retail organizations aren’t aware of these attacks happening and don’t have the resources fight back against it.

Key Findings from our Retail Dark Web Search

To help you understand how cybercriminals target retail companies, we've searched the Dark Web for common tactics and examples of eCommerce scams. Here's what we found.

Individual Suppliers

Using the Dark Web, individuals can now become independent suppliers by developing tools that enable them to buy the entire stock of a product from an eCommerce shop and then sell that item for more money (see Figure 1). Once a hacker has bought all the units of a popular product, consumers have no other options but to buy it from the hacker. And because fads and product obsession drive such high demand, this tactic usually works.



[redacted] WEBSITE SITEKEY EXTRACTION SCRIPT – COP [redacted]

Day 29 Hrs 23 Min 19 Sec 28

Available QTY 49 items

Buy Now $100.00 (Reference Only)

0.009 BTC

0.560 LTC

Item ID	#1008726	Category:	Bots
Condition	Brand New	Location:	USA
Ending	2/16/2018, 8:39:57 PM	Viewed:	5 times
Watch List	+ Watch		

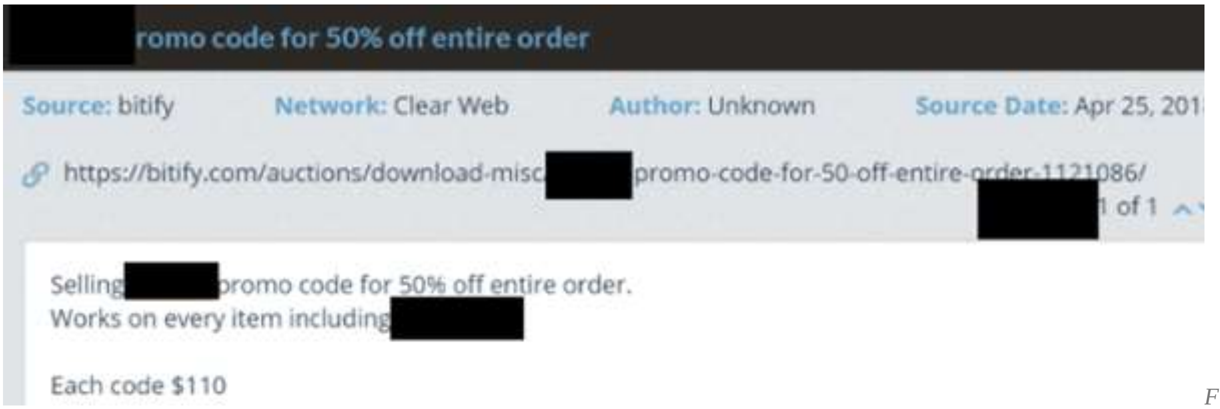
Item description

For those of you who know the insane profits that come with reselling [redacted] sneakers, this is something required to be able to be successful in purchasing the limited shoes. [redacted] literally sell out in a matter of a couple minutes if not more likely in seconds. It took me multiple years to accumulate the tools to be successful buying these shoes. If your wondering why, its because you can easily make $500 profit for every pair that you buy. That profit is actually on the low side of the average believe it or not. Im listing multiple tools that are all very much needed to have a prayer at successfully buying [redacted] the tool in this listing is definitely one of those required. Included in your purchase is a step-by-step guide for setup and usage of the script your purchasing. Im only selling a liimited number of each of the tools so dont wait, people are literallly making a lavish living buying and reselling this particular shoe alone.

Figure 1: Example of Item Being Re-Sold on Illegal Online Market

Most of these items can be found in the Black Markets; however, the integrity of these posts are questionable at best. The hackers don't always have the intention of giving you your money's worth once you've paid. Some of these published posts are scams, where they'll take your money and either send you a knock-off version or not send you anything at all.

Trading Promo Codes



[redacted] romo code for 50% off entire order

Source: bitify Network: Clear Web Author: Unknown Source Date: Apr 25, 201

https://bitify.com/auctions/download-misc[redacted]promo-code-for-50-off-entire-order-1121086/

[redacted] 1 of 1

Selling [redacted] promo code for 50% off entire order.
Works on every item including [redacted]

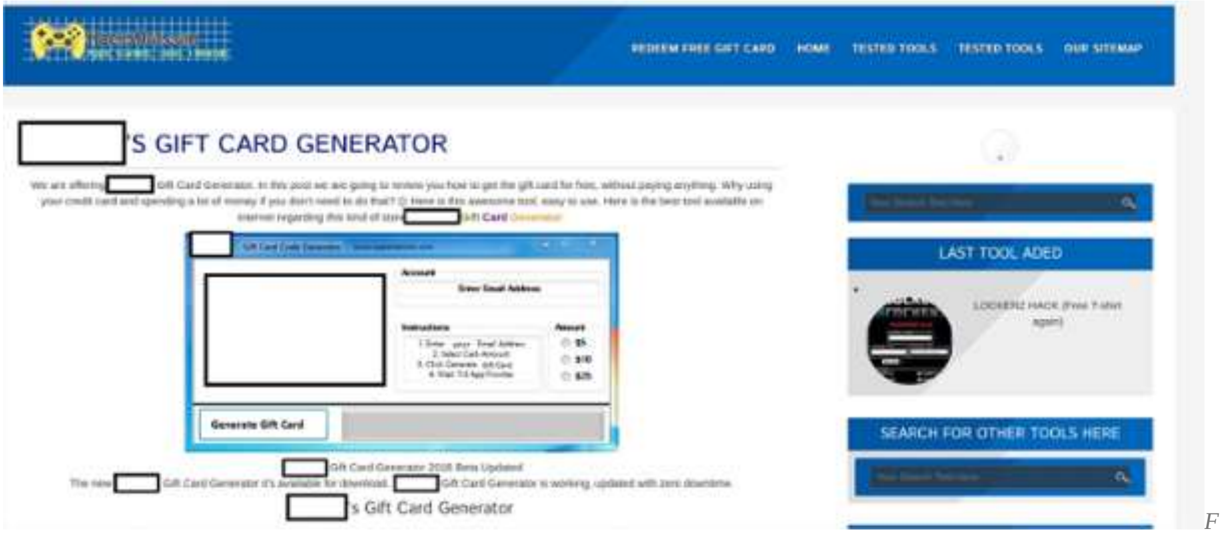
Each code $110

Figure 2: Example of Promo Codes for Sale

Retail products are not the only thing that you can find in the Dark Web. Hackers often sell other items, such as gift cards and promo codes (see Figure 2). Another common tactic is developing a mechanism to create gift cards for popular brands on their own (see Figures 3 and 4). This tool is known as gift card generator and it it a relatively new service hackers offer in dark web forums.

Every gift card uses an ID number which ties back to an account in the retailer's database. These gift card generators use a bot that generates ID numbers, checks their validity against public algorithms, and then finally checks to see if they have a balance remaining. They can then sell these gift card balances for profit or use them to buy their own goods, which they will later sell on their own. As you might expect, these gift card generators can be very unreliable and are often just scams setup to get users to buy gift cards that don't actually work.

For this type of scheme, it doesn't matter how hackers obtain these gift cards, whether it's buying them at a discount, stealing them from a company database, or developing a mechanism to create gift cards on their own. All of these tactics can significantly eat into a company's profits and damage brand reputation.



[redacted]'S GIFT CARD GENERATOR

We are offering [redacted] Gift Card Generator. In this post we are going to review you how to get the gift card for free, without paying anything. Why using your credit card and spending a lot of money if you don't need to do that? ☺ Here is this awesome tool, easy to use. Here is the best tool available on internet regarding this kind of stuff [redacted] Gift Card Generator

[redacted] Gift Card Code Generator

[redacted]

Account: Enter Email Address

Instructions
1. Enter your Email Address
2. Select Card Amount
3. Click Generate Gift Card
4. Wait Till App Finishes

Amount
○ $5
○ $10
○ $25

Generate Gift Card

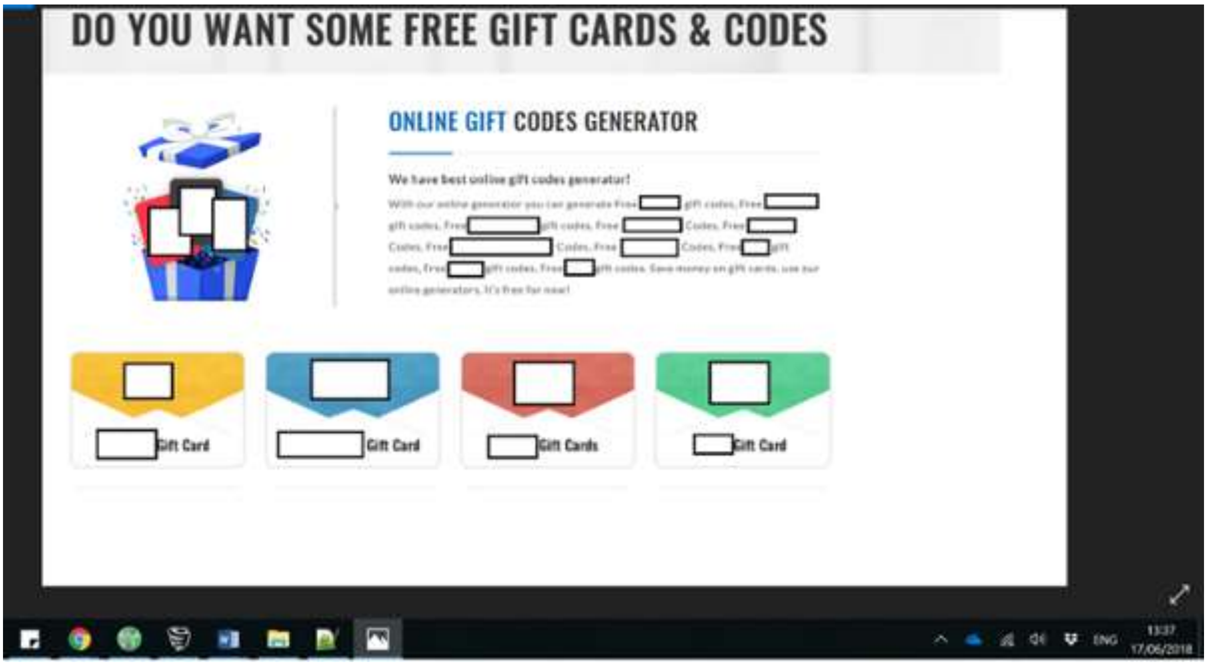
[redacted] Gift Card Generator 2018 Beta Updated

The new [redacted] Gift Card Generator it's available for download. [redacted] Gift Card Generator is working, updated with zero downtime.

[redacted]'s Gift Card Generator

LAST TOOL ADED
LOCKERZ HACK (Free T-shirt again)
SEARCH FOR OTHER TOOLS HERE

Figure 3: Example of a Gift Card Generator for Popular Food Retailer



DO YOU WANT SOME FREE GIFT CARDS & CODES

ONLINE GIFT CODES GENERATOR

We have best online gift codes generator!

With our online generator you can generate Free [redacted] gift codes, Free [redacted] gift codes, Free [redacted] gift codes, Free [redacted] Codes, Free [redacted] Codes, Free [redacted] Codes, Free [redacted] Codes, Free [redacted] gift codes, Free [redacted] gift codes, Free [redacted] gift codes. Save money on gift cards, use our online generators. It's free for now!

[redacted]
[redacted] Gift Card

[redacted]
[redacted] Gift Card

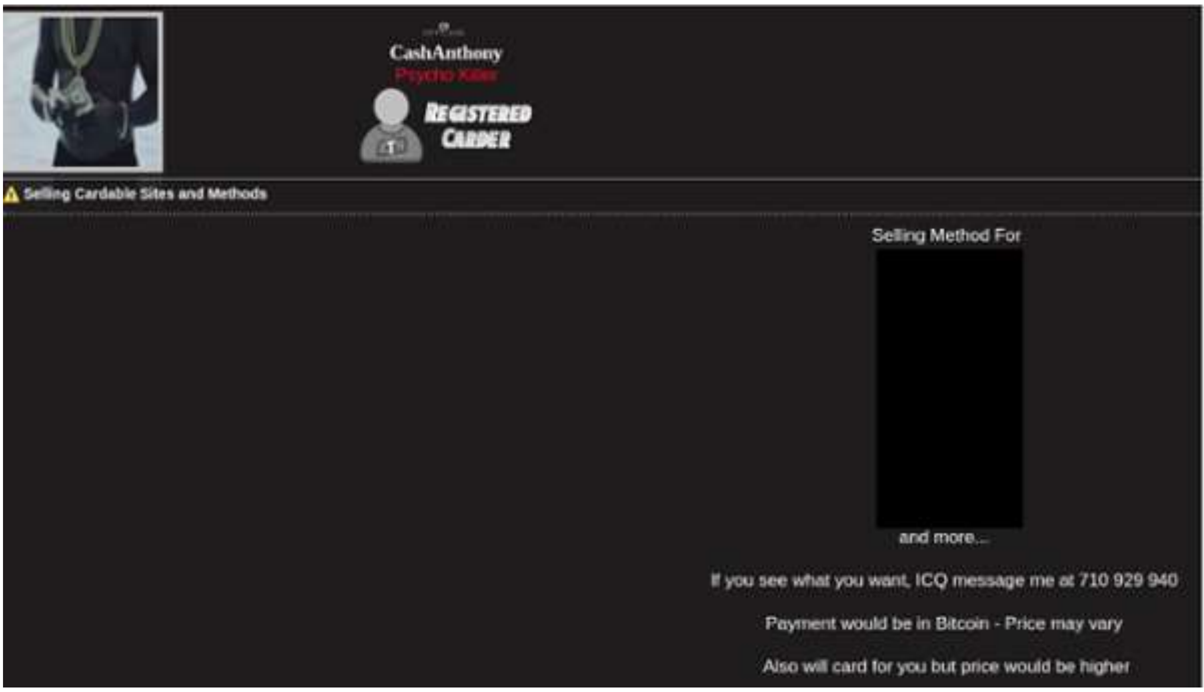
[redacted]
[redacted] Gift Cards

[redacted]
[redacted] Gift Card

Figure 4: Example of Gift Card Generator

Carding Methods

Another bit of information hackers trade on retail companies is carding methods. Carding methods are tactics to help you manipulate the details of someone else's credit card to your advantage. Many hackers sell carding methods on retail companies so other hackers can buy products with stolen credit cards and not get caught (see Figure 5).



Selling Cardable Sites and Methods

Selling Method For

[redacted]

and more...

If you see what you want, ICQ message me at 710 929 940

Payment would be in Bitcoin - Price may vary

Also will card for you but price would be higher

Figure 5: Example of a Carding Method Sold on the Dark Web

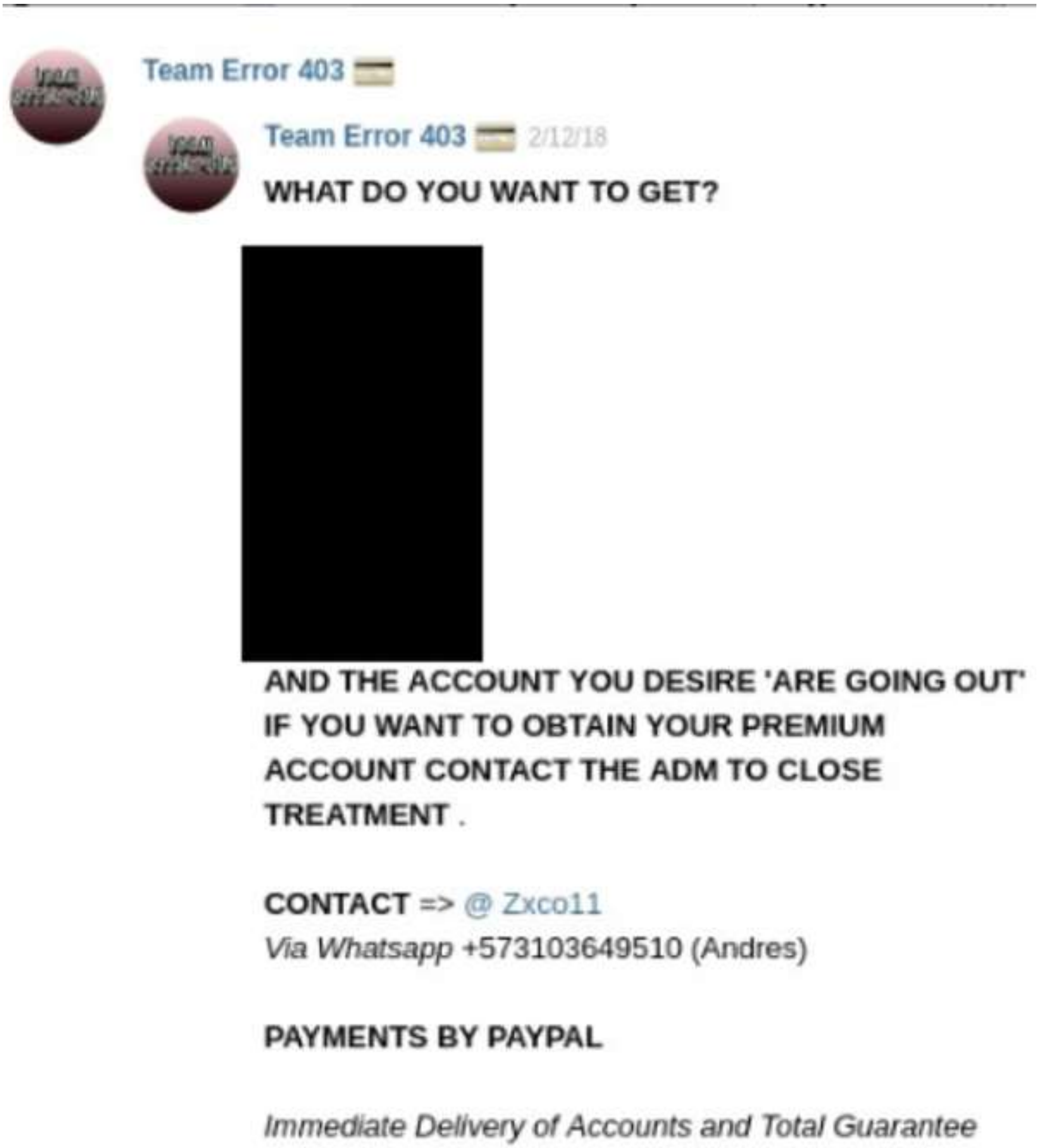
Premium Users

Finally, you can also find instances of hackers selling the account details of "Premium Users" on the Dark Web. A premium user account is an account that has achieved some sort of benefit or reward status on the retailer's site due to their buying activities.

Many retail and eCommerce companies decide to reward a user that is active on their site by giving them points for every purchase they make. The user can later use these points to purchase other items on the retailer's site. However, these "Premium Users" have become popular targets for hackers. If a hacker gains access to a user's account, they can use that in a number of different ways, like:

- Selling the user's login information online
- Selling the user's points
- Using the points to buy "free" goods they can later sell for a profit

In addition, because people typically use similar passwords for their different accounts, a hacker can likely guess the login information for other sites to continue exploiting this "Premium User".



Team Error 403

Team Error 403 2/12/18

WHAT DO YOU WANT TO GET?

[redacted]

AND THE ACCOUNT YOU DESIRE 'ARE GOING OUT' IF YOU WANT TO OBTAIN YOUR PREMIUM ACCOUNT CONTACT THE ADM TO CLOSE TREATMENT .

CONTACT => @ Zxco11
Via Whatsapp +573103649510 (Andres)

PAYMENTS BY PAYPAL

Immediate Delivery of Accounts and Total Guarantee

Figure 6: Example of a “Premium User” account for sale on the Dark Web

Conclusion

Although retail companies are fairly new targets for criminals, the profits they can generate are huge due to the increasing number of eCommerce transactions. It’s become incredibly easy for cybercriminals to run schemes the exploit both retailers and consumers, and as a result, they’ve been able to build a highly profitable revenue source.

Retail organizations need to be aware of these tactics and monitor for them on the Dark Web. Leveraging Dark Web reconnaissance can help you identify retail schemes before they’re carried out. Not only will this protect your profit margins, but will help you protect your customers as well, helping you maintain (or even strengthen) your brand credibility and reputation.

Want to learn more about how hackers buy and sell information on Dark Web Black Market forums?

How Digital Risk Protection Helps You Reduce Your Organization’s Attack Surface

by Nathan Teplow / June 12, 2018

INTSIGHTS

Threat Intelligence Realized.

The Internet Never For

How to Reduce Your Or
Attack Surface and Cyb
Digital Risk Reconnaissa

In our modern age of digital connections and ubiquitous Internet access, both organizations and individuals face a “double-edged sword” when using web-based technologies. As we’ve increased our usage of the World Wide Web, our digital footprints have grown exponentially, and as a result, so has the digital attack surface. This has given cyber criminals a vast network of information to leverage for carrying out increasingly targeted and effective attacks.

For companies, “Footprint Reconnaissance” (i.e. monitoring and tracking your digital footprint over time) has become a serious challenge. Most organizations have numerous web outlets, social media accounts, servers, IP ranges, ASN’s, databases, repositories, cloud storage servers and other Internet-facing assets. And these are just the resources that the security and/or IT department typically know about. There are usually many more assets that the company doesn't know about, like ad-hoc sites and services, temporary QA environments (which too often stay permanent), and all types of Internet-facing services, which likely were set up by former employees, but are now forgotten.

The Rise of the Digital Risk Protection (DRP) Market

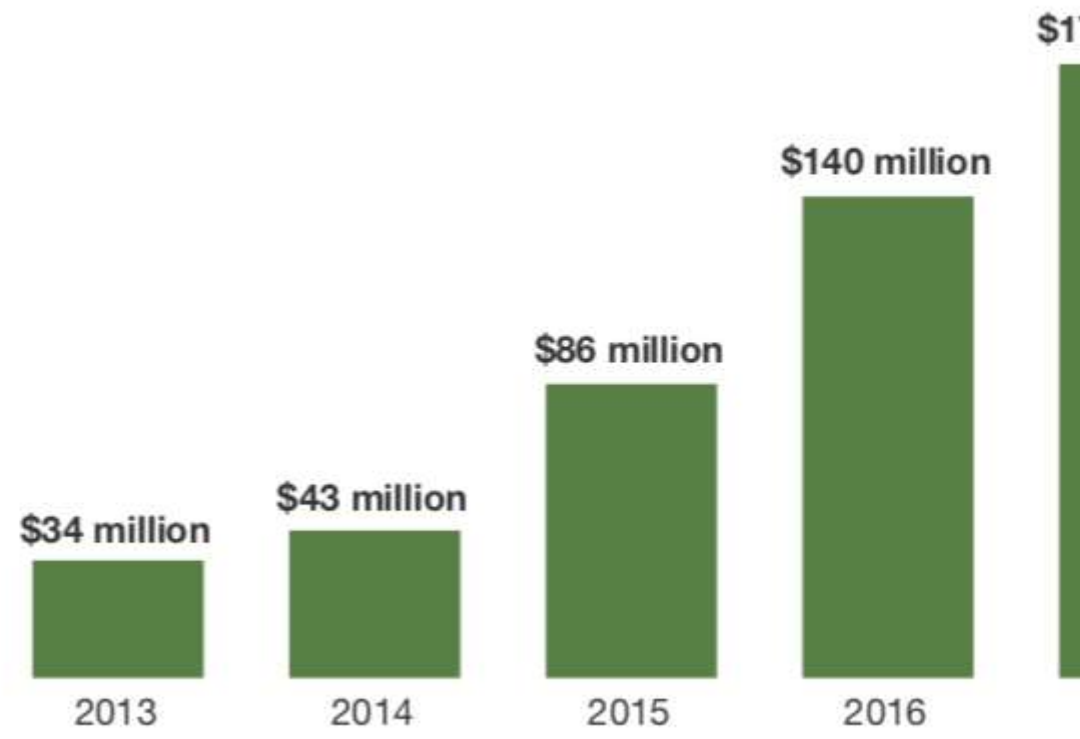
As digital footprints widen, security pros — as well as marketing, PR, and other peers — are seeking DRP solutions to better monitor and mitigate digital risk. DRP adoption is steadily rising because these tools can help:

- Discover and monitor all digitally exposed infrastructure and assets
- Minimize the organization’s mean-time-to-remediate (MTTR) issues
- Strengthen customers’ trust in the brand

As a result, many venture capitalists have begun investing in the DRP market. According to Forrester’s new report, *Digital Risk Protection, Q2 2018*, VC’s have invested nearly $500 Million in DRP vendors since 2013, with investments reaching over $179 Million in 2017. While investment has increased, M&A in the market remains relatively quiet as most DRP vendors focus on organic growth.

FIGURE 1 VC Funding In Digital Risk Protection Vendors Since 2013

DRP funding by year



Source: Forrester Research and Venture Scanner

Digital Risk Protection Market Overview

In Forrester's recently published research report, *Digital Risk Protection, Q2 2018*, they provide an overview of 21 DRP solutions. The report breaks these solutions down into three core functions: mapping, monitoring, and mitigating. Each category of vendor has capabilities that align primarily with one of these three objectives:

- Digital footprint mapping tools track firms' digital assets and infrastructure
- Digital risk reconnaissance tools uncover firms' digital risk exposure
- Digital risk defense tools prevent or resolve attempts to abuse firms' digital presence

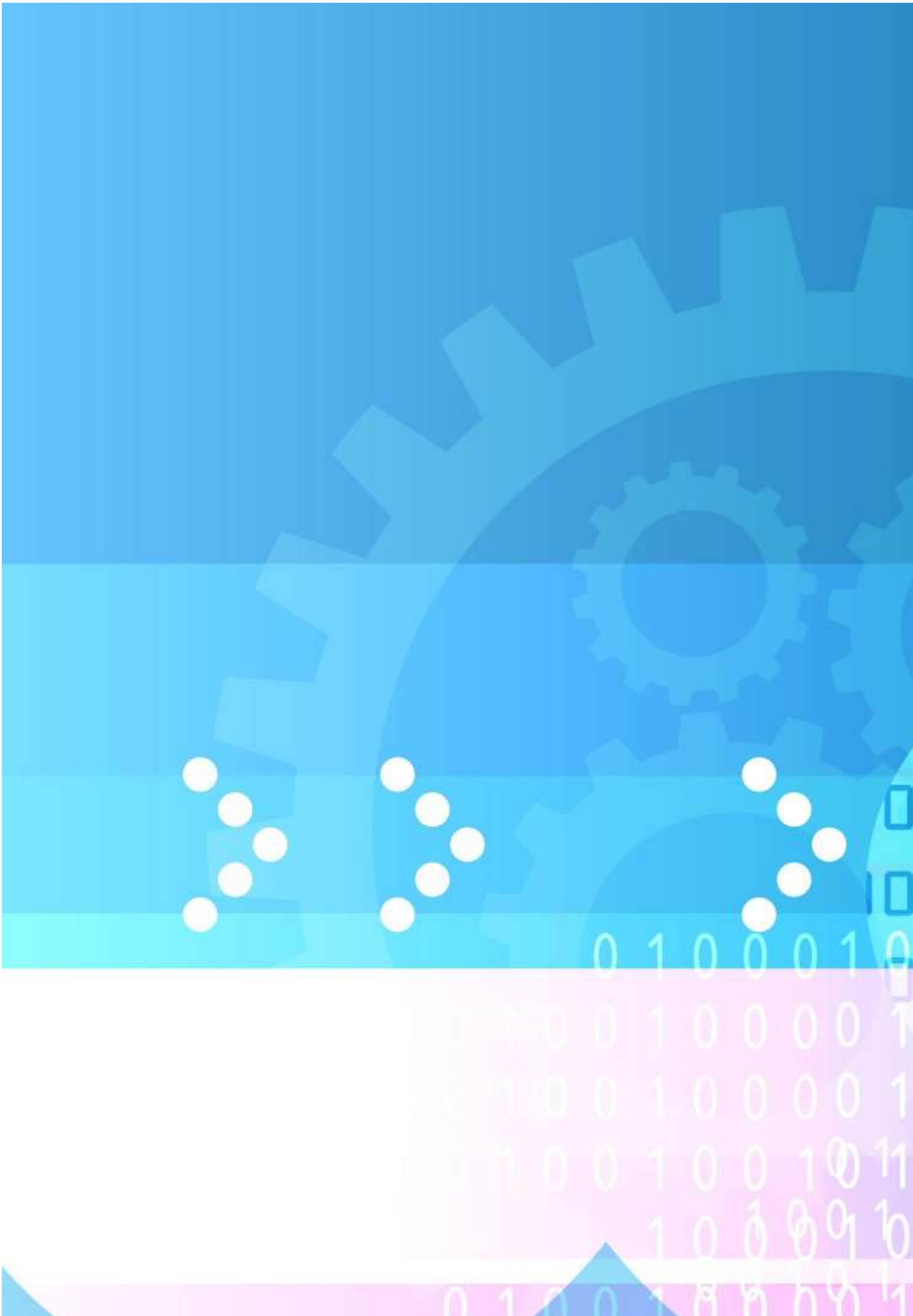
IntSights is proud to sponsor this year's Forrester report and be featured as a Growth Vendor. In the report, you can find a foreword from IntSights on how organizations can reduce their digital footprint with Digital Risk Protection, as well as Forrester's analysis of the DRP market.

Download the Full Forrester *Digital Risk Protection, Q2 2018* Report

Download Now

How to Identify and Thwart Phishing Attacks Against Your Customers and Employees

by Nathan Teplow / June 21, 2018



Phishing is a popular social engineering tactic used by hackers, typically intended to dupe users into clicking on a link, opening a malicious file and/or giving away some sort of personal info. Sometimes the phishing attempt is the primary goal of the attack, like tricking a user to download ransomware. Other times, it's part of a larger attack, like having someone submit their credentials on a fake login site, allowing the hacker to use them later to access confidential data.

In either scenario, phishing attacks can be very effective at targeting both employees and customers because hackers often use popular brands to trick users. This can be a major challenge for companies, because it's their responsibility to keep their customers safe, yet they have little control over how hackers might use their brand to run phishing schemes.

Here is how you can help identify and take down phishing attacks before they are ever launched against your customers or your employees.

Identifying Phishing Attacks in the Planning Phase

In order to stop phishing attacks, organizations must use the planning phase to their advantage. Hackers often collect information about their targets using Dark Web forums in order to make their attacks more targeted and successful. By monitoring sources across the surface, deep and dark web, you can identify these key indicators of phishing attacks, enabling you to prepare your organization and take down phishing attempts before they are carried out.

Common Phishing Attack Indications

So what should you monitor for in order to identify and take down phishing attacks? Here are some common indicators that your organization is being targeted.

Suspicious Domain Registered (Bonus: MX Records Added)

Every phishing attack needs to use a domain name in order to send an email and/or deliver a malicious payload. Cybercriminals often use domain names that are similar to popular brands or websites (for example, amazonn.com) in order to appear legitimate. As an organization, you need to know when domains similar to yours are registered, as they are key steps in the phishing attack process.

In addition, if MX records are added, that typically indicates the domain will be used to send emails, which is another key indication the domain may be used in a phishing attack.

To protect your customers and employees, you need to have some sort of monitoring process in place to track when similar domains are registered and if MX records are added. If a potential phishing domain is registered, be sure to block that domain in your URL filtering system and work with the registrar to take it down before it's used in an attack.

Fake Email Address

The key to a successful phishing attack is getting the user to believe an email is legitimate and engage with it in some way. Hackers often do this by mimicking key employees (like the CEO for an employee attack) or popular brands (for a "consumer" attack). Therefore, companies should also monitor for fake email addresses that use key employee or executive names (e.g. CEO's name), or email addresses that use brand names (e.g. FedEx Shipping Notification).

If one of these addresses is discovered, be sure to block the domain in your mail relay system and again, work with the registrar to have the domain taken down.

Fake Mobile Application or Social Media Account

While email is a popular attack vector for phishing schemes, it's not the only one. More recently, hackers have started using social media and mobile app stores to impersonate popular brands and trick users into giving away their information.

Users aren't always careful with what applications they download or which social media pages they engage with, and as a result, this has become an increasingly successful attack vector for cybercriminals.\

Companies need to monitor various social media sites to identify fake pages and alert the site if one is found. Additionally, they should monitor mobile app stores, especially the non-official app stores, to look for and take down fake mobile applications using their brand.

Leaked Employee Credentials

There is no shortage of leaked credentials these days across the dark web. Not only do hackers use these credentials to access corporate systems and confidential information, they can also be used to send phishing emails to employees within the organization. For example, if a hacker wants to install malware on a CEO's computer, rather than sending them an email from a phishing domain, they may try to purchase an employee's email credentials on the dark web in order to send the CEO a malicious link. Alternatively, they may try to phish email credentials from employees in order to access their email account.

These types of phishing attacks can be very successful because email systems don't typically block emails from within the organization.

Leaked credentials are often used as the starting point of a phishing attack. Therefore, organizations need to monitor the dark web for leaked employee credentials. Not only will this help you protect against phishing attacks, but will help you lock down other potentially accessible systems and even identify potential leaks in your organization.

Employees on Phishing Target List

Phishing attacks aren't always planned in complete isolation. Hackers sometimes post target lists for phishing attacks on dark web forums to coordinate and plan their attacks. Identifying these lists can help you identify who and how an attacker may be planning to launch a phishing attack. In addition, a hacker might solicit help building a website for a phishing campaign, or may even purchase a ransomware program to use in their attacks.

Organizations should monitor dark web forums for these common indications of a planned phishing attack.

Conclusion

Phishing is a fairly simple, yet effective tactic used by hackers, and we've seen plenty of creativity in how they attempt to trick users into clicking a link or opening a file. Organizations have a responsibility to their customers to protect them against phishing attacks, even if the organization is not to blame for the attack. However, the planning and coordination of phishing attacks can be used as an advantage. Organizations need to monitor for these key indicators of phishing attacks in order to proactively protect their employees and their customers.

11 Infamous Dark Web Black Market Avatars, Groups and Users

by Itay Kozuch / June 19, 2018

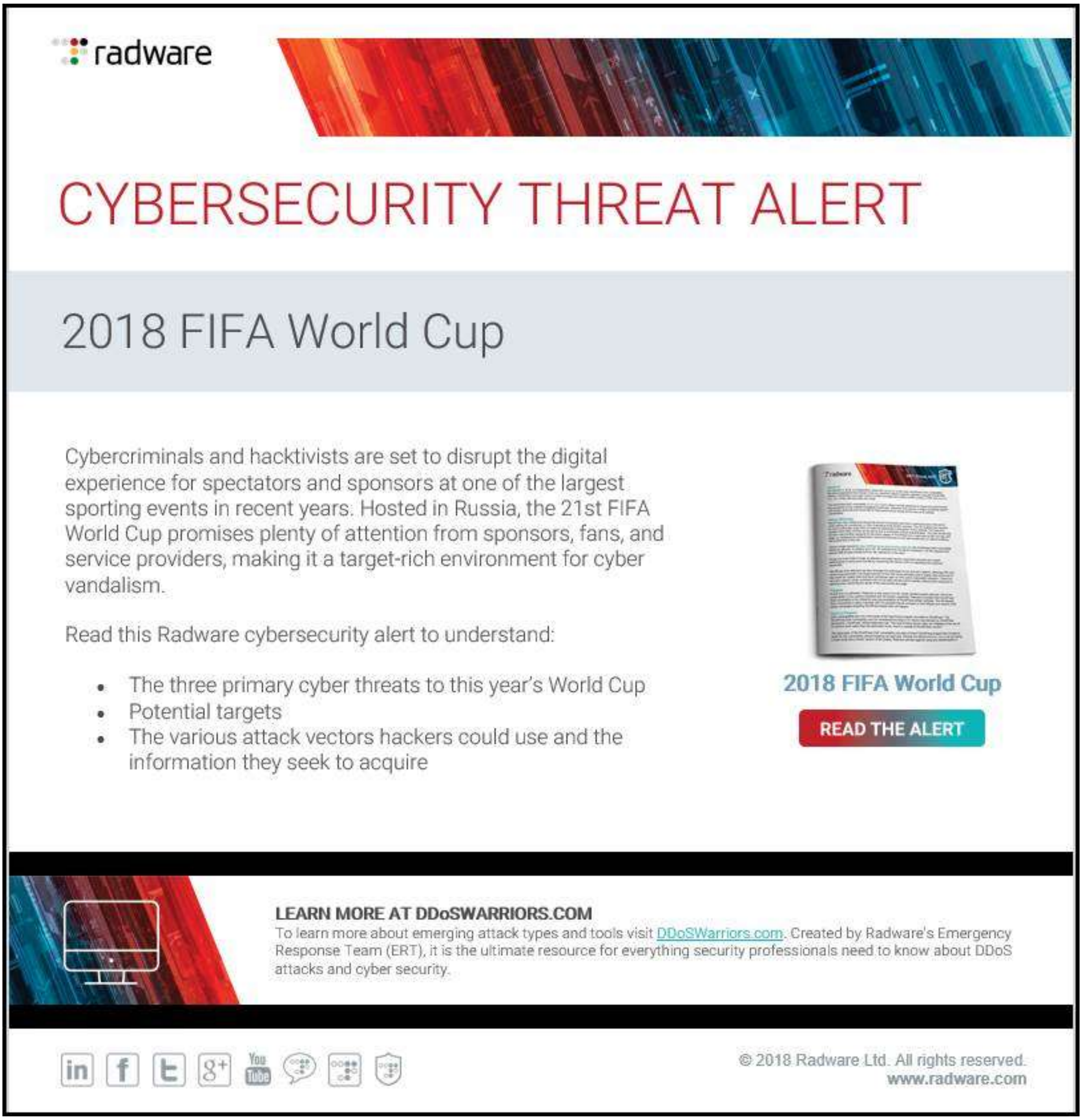
Anonymous web browsers (like Tor and I2P) have created what has become known as the Dark Web, enabling users to access and host websites completely anonymously. Naturally, this has given rise to a large community of underground illegal black markets and forums, where users can buy or sell almost anything, including weapons, drugs, confidential data and other illegal services.

Just like today's most popular eCommerce or review sites have power users and well-known reviewers, dark web black markets have developed quite a few famous (or perhaps infamous) power users.

Here is our list of 11 of the most infamous dark web black market avatars, groups and users.

1. **Astrid**: Creator and Moderator of various Dark Web markets. They are considered very promiscuous, having had relations with all Moderators there, and also is the CSS guru!
2. **Avengers**: A group of individuals who are well known for ordering LSD from various vendors back in the days of Silk Road 1.0. This group would reagent test it, consume it, and write reviews about the quality of the LSD products.
3. **Backopy**: The Administrator of Black Market Reloaded (BMR). BMR is the oldest Dark Web market (since the Silk Road was shut down). BMR is currently offline with plans to relaunch with a newer version.
4. **Cirrus**: A Silk Road forum moderator.
5. **Defcon**: The alias of the Silk Road 2.0 Admin. A person named Blake Benthall was arrested During Operation Onymous and is alleged to be Defcon.
6. **Digitalink**: AKA Jacob Theodore George IV, according to Homeland Security Investigations (HSI). Digitalink was the first vendor on Silk Road selling illegal drugs to be arrested.
7. **Dread Pirate Roberts (Ross William Ulbricht)**: The pseudonym used by the creator and administrator of the original Silk Road market. It has been speculated that more than one person may have been using this pseudonym, but "Ross William Ulbricht" was identified by the FBI as being the only owner. He was an Eagle Scout and a known libertarian. The original Silk Road website went down after his arrest.
8. **Flush (Curtis Green)**: An individual the FBI accused Dread Pirate Roberts of ordering to be murdered. This person is also accused of being 'Chronicpain' from the Silk Road Forums, and an employee of Silk Road.
9. **Libertas**: Pseudonym used by one of the original Silk Road forum administrators, and also used by one of the administrators of Silk Road 2.0. Libertas was arrested by the "Garda Siochana" (Irish police).
10. **Lucyskyhigher**: A Reddit community (moderated by sexiest biotch) that features an informative and largely humorous gathering place for all dark web markets.
11. **Tony76**: Was a trusted vendor on the original Silk Road, then ran a massive "Finalize Early (FE)" scam. The FBI accused Dread Pirate Roberts of placing a hit on the individual using this pseudonym. He scammed a large number of Silk Road users, but his true identity and the details of if he was killed or not are still unclear.

You can access this report by clicking here.



radware

CYBERSECURITY THREAT ALERT

2018 FIFA World Cup

Cybercriminals and hacktivists are set to disrupt the digital experience for spectators and sponsors at one of the largest sporting events in recent years. Hosted in Russia, the 21st FIFA World Cup promises plenty of attention from sponsors, fans, and service providers, making it a target-rich environment for cyber vandalism.

Read this Radware cybersecurity alert to understand:

- The three primary cyber threats to this year's World Cup
- Potential targets
- The various attack vectors hackers could use and the information they seek to acquire

2018 FIFA World Cup

READ THE ALERT

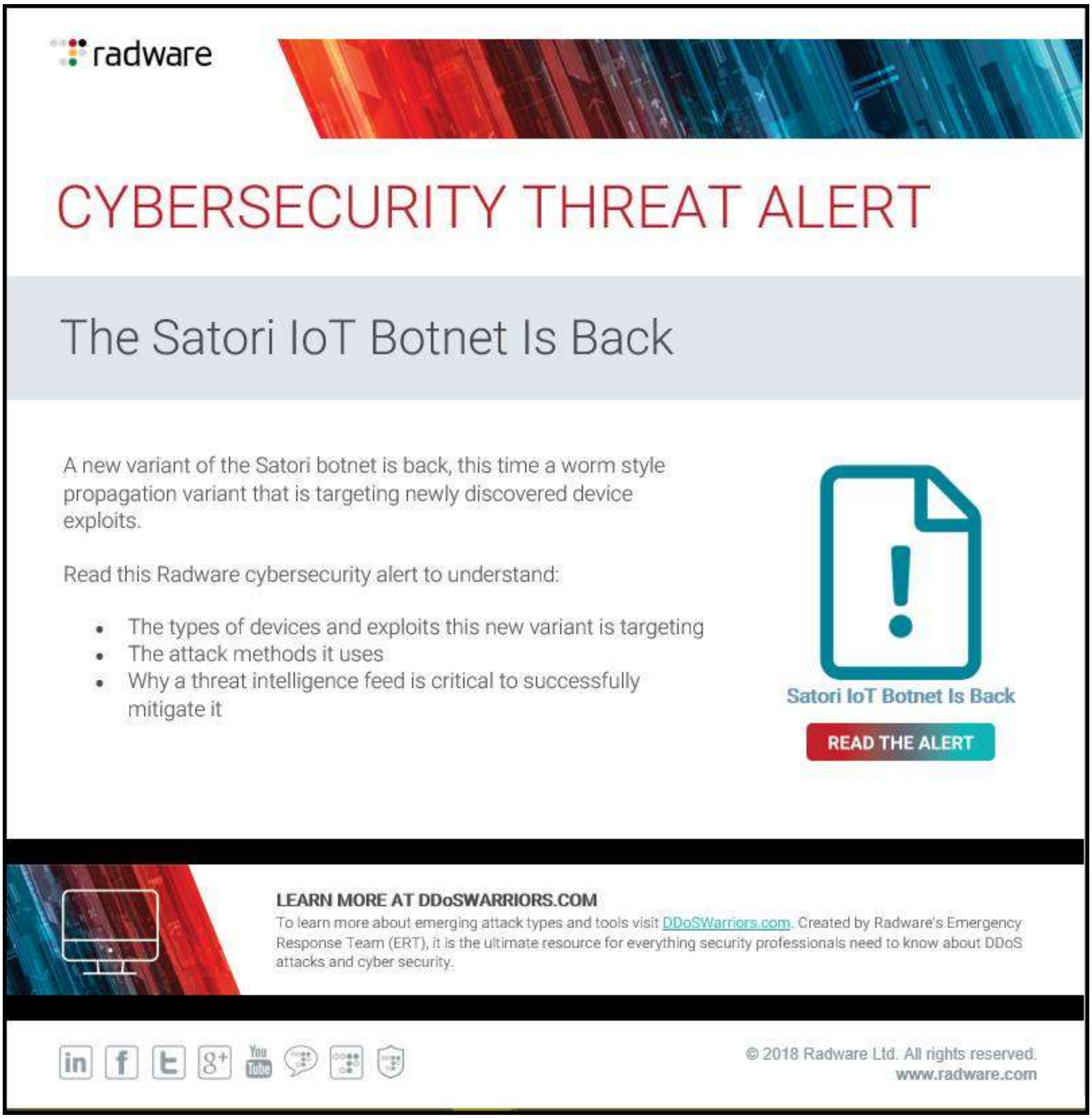
LEARN MORE AT DDoSWARRIORS.COM

To learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

© 2018 Radware Ltd. All rights reserved.
www.radware.com

The Satori IoT Botnet Is back. The report can be found at: https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/satori-iot-botnet/

Feel free to leverage this alert in your conversations with your clients, hopefully to inspire a Radware conversation/meeting.



radware

CYBERSECURITY THREAT ALERT

The Satori IoT Botnet Is Back

A new variant of the Satori botnet is back, this time a worm style propagation variant that is targeting newly discovered device exploits.

Read this Radware cybersecurity alert to understand:

- The types of devices and exploits this new variant is targeting
- The attack methods it uses
- Why a threat intelligence feed is critical to successfully mitigate it

Satori IoT Botnet Is Back

READ THE ALERT

LEARN MORE AT DDoSWARRIORS.COM

To learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

© 2018 Radware Ltd. All rights reserved.
www.radware.com

Radware's Web Application Firewall Just Got Better

Radware's web application firewall (WAF) solutions help ensure fast, reliable, secure delivery of mission-critical web applications for organizations worldwide. Our WAF technology is available through AppWall, an on-premise WAF or Cloud WAF Service, and is recommended by NSS Labs, is certified by ICSA Labs and is PCI compliant. It combines both positive and negative security models to provide complete protection against web application attacks (injections, XSS, CSRF), bot attacks, CDN-based assaults, API exploitations, HTTP/S attacks, DoS, Brute Force attacks on login pages and more.

Take a look at the updated sales and marketing materials to understand market trends and the increasing demand for specific use cases, such as bot management and mitigation, API security and denial of service.

Learn More

- New! Web Application Security🔒
- New! Radware WAF Technology vs. the New OWASP Top 10🔒
- Radware Web Application Security Study🔒
- AppWall Battle Card🔒
- Cloud WAF Service Battle Card🔒
- Updated! AppWall — More Than Just a WAF🔒
- WAF Auto-Policy Generation🔒

Technical White Papers

- The Technology Behind Radware's Web Application Security Solutions
- Creating a Safe Environment for Underprotected APIs
- Integrated Hybrid Protection Against Application Layer DoS

Security Update Subscription (SUS) for AppWall Customers

Radware’s Emergency Response Team SUS is a security advisory and managed monitoring/detection system dedicated to protecting applications and APIs against the latest vulnerabilities and threats, such as the OWASP Top 10. The service delivers rapid and continuous updates to current subscribers.

SUS complements AppWall’s protection against known and new threats by providing various types of data, including geolocation database updates that provide role-based policies for clients accessing from different geographies. Other components include attack signatures for various attack vectors:

INJECTION ATTACKS	ACCESS VIOLATIONS	DATA LEAKAGE	XSS AND RFI/LFI
SQL and NoSQL injection Mail command injection Null byte injection XPath injection SSL injection OS command injection LDAP injection	Wrong username/password authentication Unauthorized access attempt Invalid client certificate attributes Folder access violation Application and server misconfiguration Path traversal Predictable resource location URL access violation Invalidated redirects	Credit card number leakage Social Security number leakage Cookie poisoning Server information leakage Other pattern leakage	Cross-site scripting Remote file inclusion File upload violation

Radware SUS is an annual subscription that requires 24x7 support and is a precondition for managed WAF services.

Learn More

New! Security Update Subscription for Radware AppWall Web Application Customers