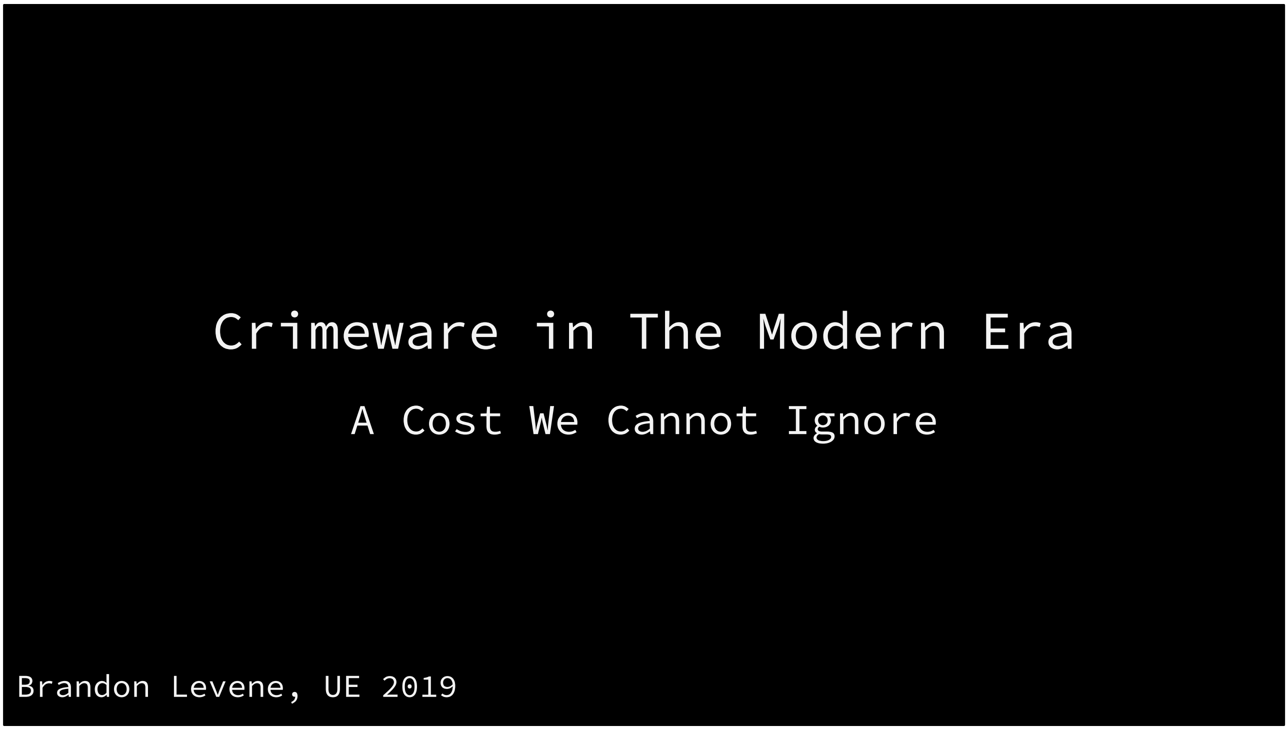
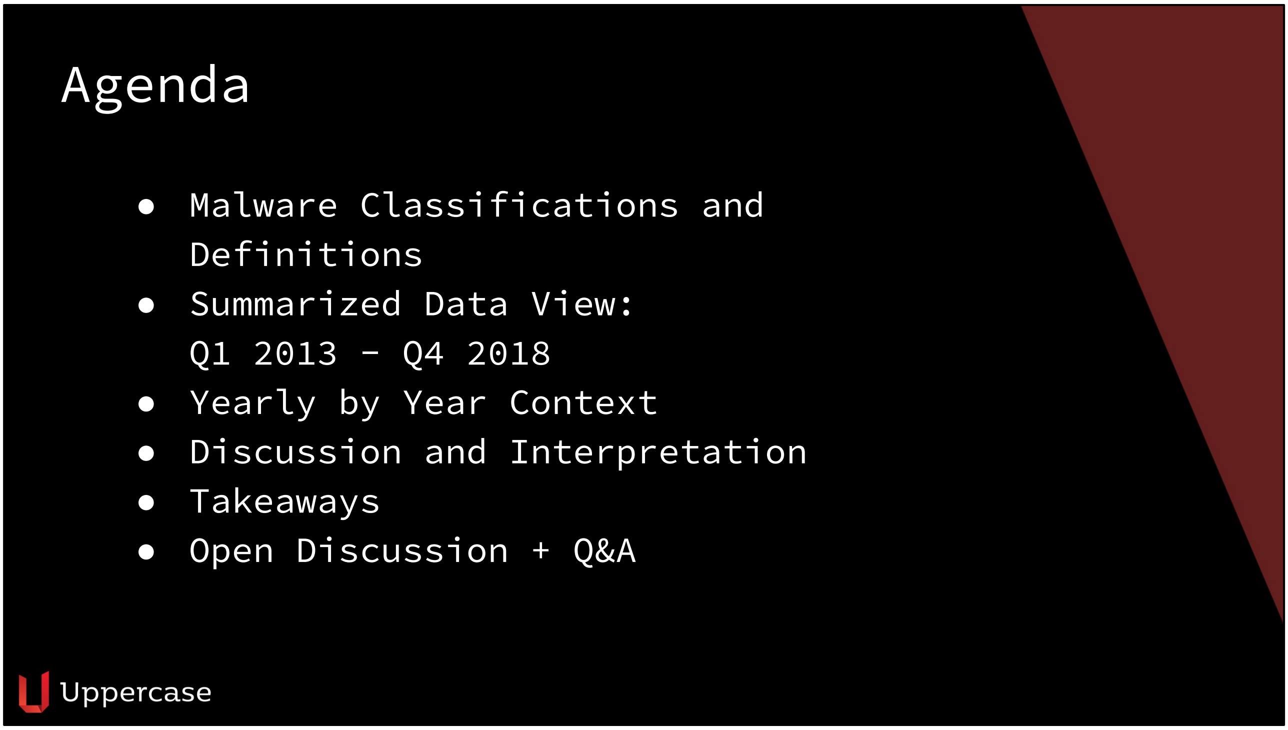


Crimeware in The Modern Era

A Cost We Cannot Ignore

Brandon Levene, UE 2019

Financially motivated malware, colloquially referred to as “crimeware,” is by far the most prevalent threat facing organizations and individuals alike. Cast aside in favor of the attention grabbing “APT,” the threat from financially-motivated threat actors is approaching nation state-levels of disruptive capability in terms of financial impact. Over the last six years, hundreds of articles, blogs, reports, and headlines have detailed the continuous evolution of tools, techniques, and procedures utilized by financially-motivated threat actors. VirusTotal is uniquely positioned to identify and analyze trends in the prevalence of different types of crimeware collected from our global community and overlay this data with the events and headlines relevant to inflection points of historic observations.

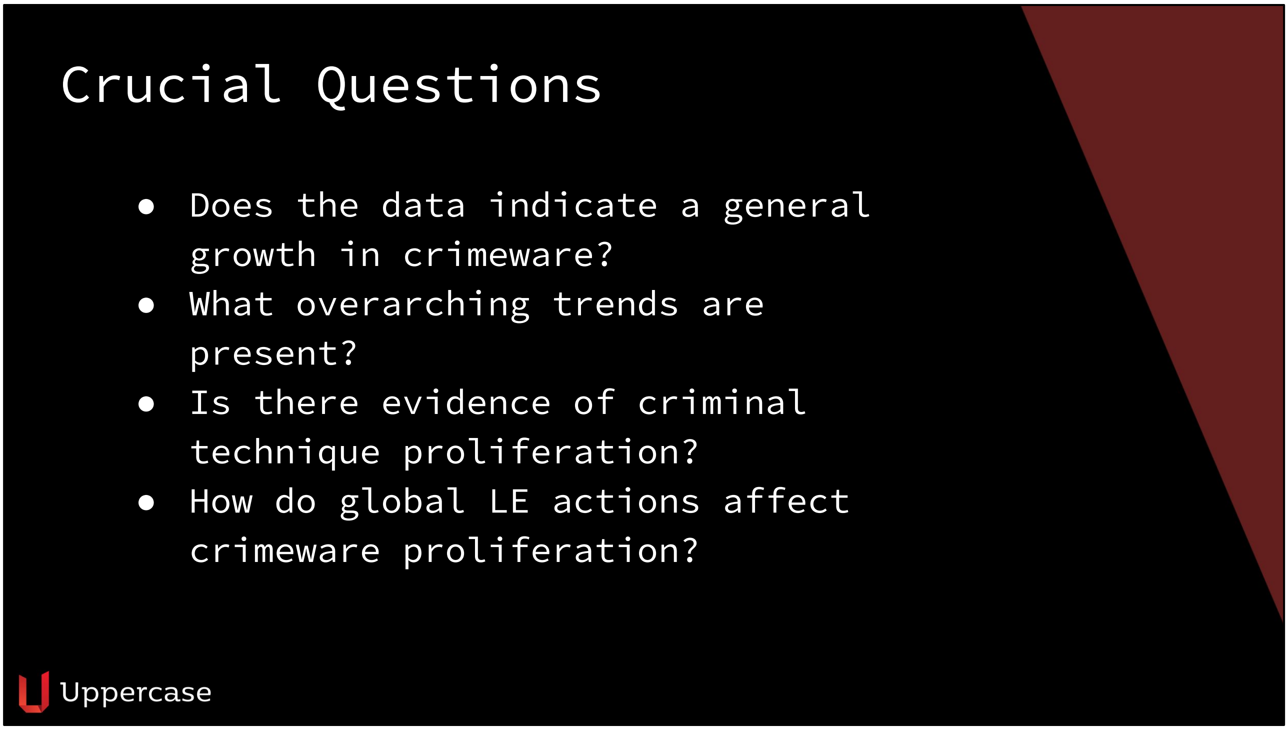


Agenda

- Malware Classifications and Definitions
- Summarized Data View:
  Q1 2013 - Q4 2018
- Yearly by Year Context
- Discussion and Interpretation
- Takeaways
- Open Discussion + Q&A

Uppercase

Malware Classifications and Definitions
Summarized Data View:
Q1 2013 - Q4 2018
Yearly by Year Context
Discussion and Interpretation
Takeaways
Open Discussion + Q&A



Crucial Questions

- Does the data indicate a general growth in crimeware?
- What overarching trends are present?
- Is there evidence of criminal technique proliferation?
- How do global LE actions affect crimeware proliferation?

Uppercase

We begin by posing a handful of crucial questions for readers to consider:

- Does the data indicate a general growth in crimeware?
- What overarching trends are present?
- Is there evidence of criminal technique proliferation?
- How do global LE actions affect crimeware proliferation?

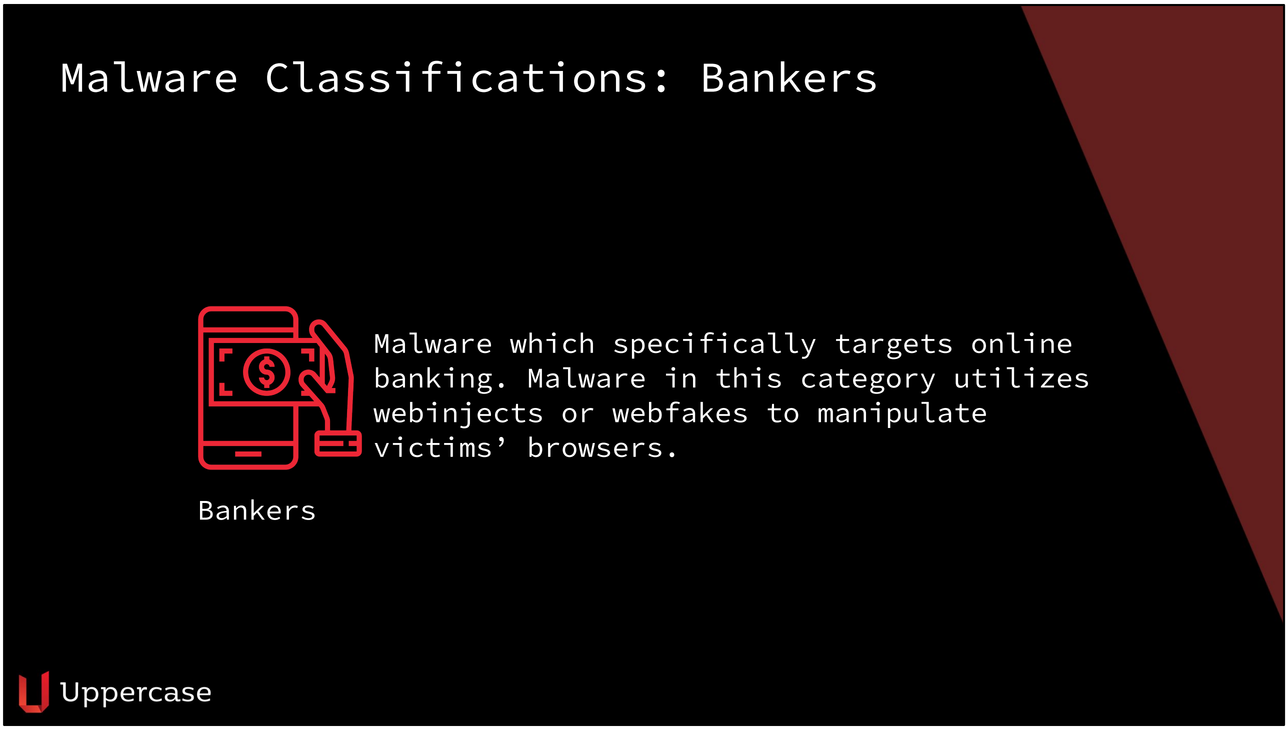
Malware Classifications

Uppercase

We have divided financially motivated malware into the following categories and definitions based on capabilities and techniques within the context of this paper

Malware Classifications

- Bankers
- Ransomware
- Infostealers
- Miners



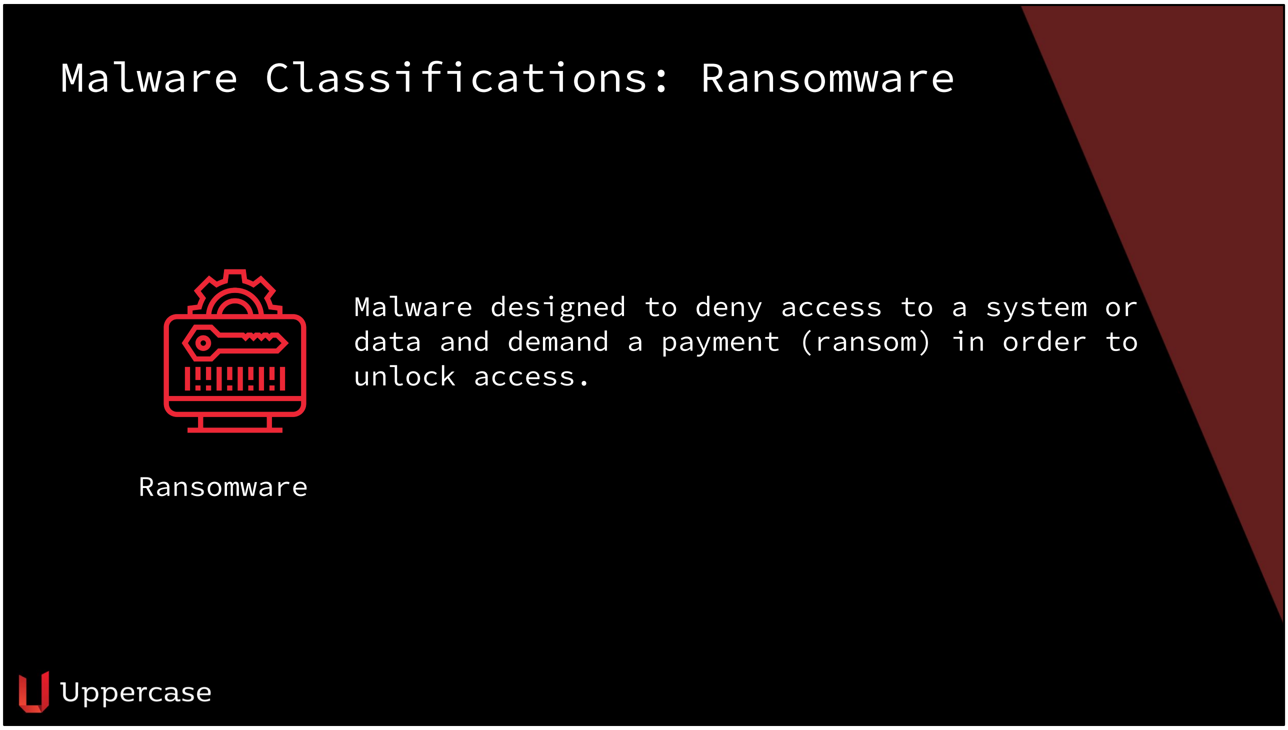
Malware Classifications: Bankers

Malware which specifically targets online banking. Malware in this category utilizes webinjects or webfakes to manipulate victims’ browsers.

Bankers

Uppercase

- Malware which specifically targets online banking. Malware in this category utilizes webinjects or webfakes to manipulate victims’ browsers.



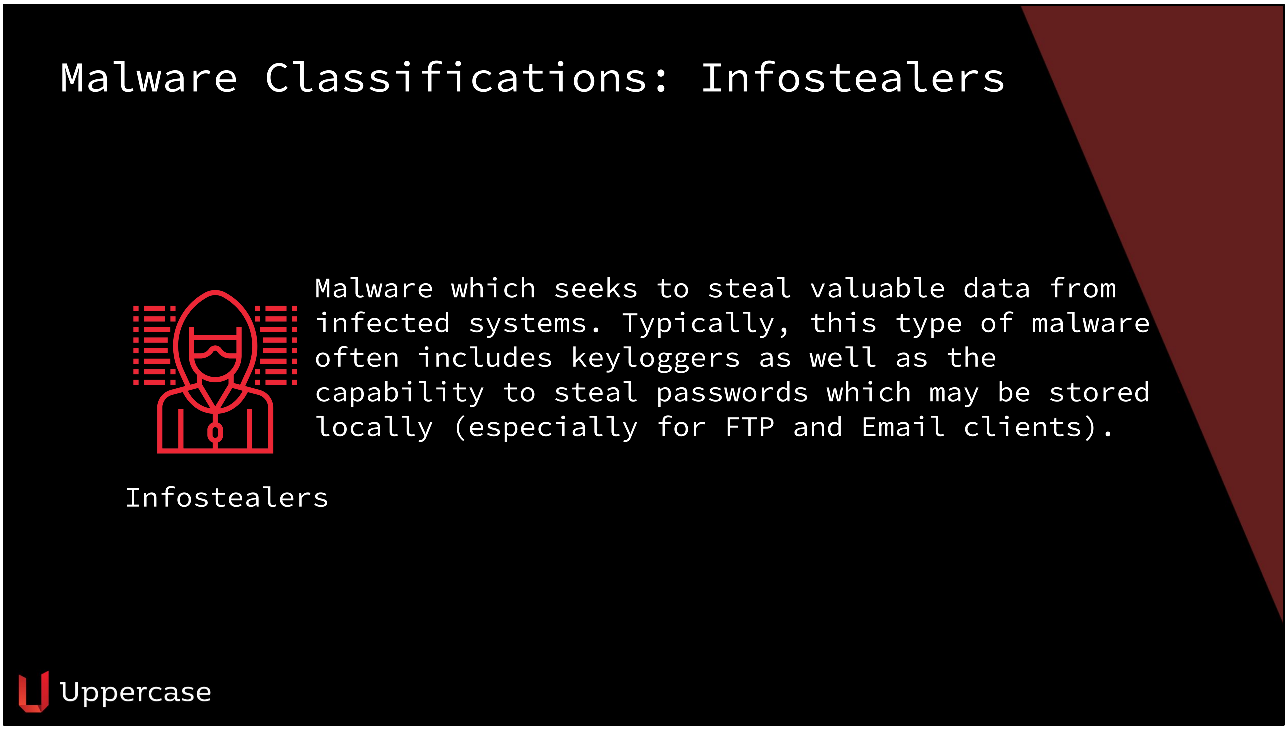
Malware Classifications: Ransomware

Malware designed to deny access to a system or data and demand a payment (ransom) in order to unlock access.

Ransomware

Uppercase

- Malware designed to deny access to a system or data and demand a payment (ransom) in order to unlock access



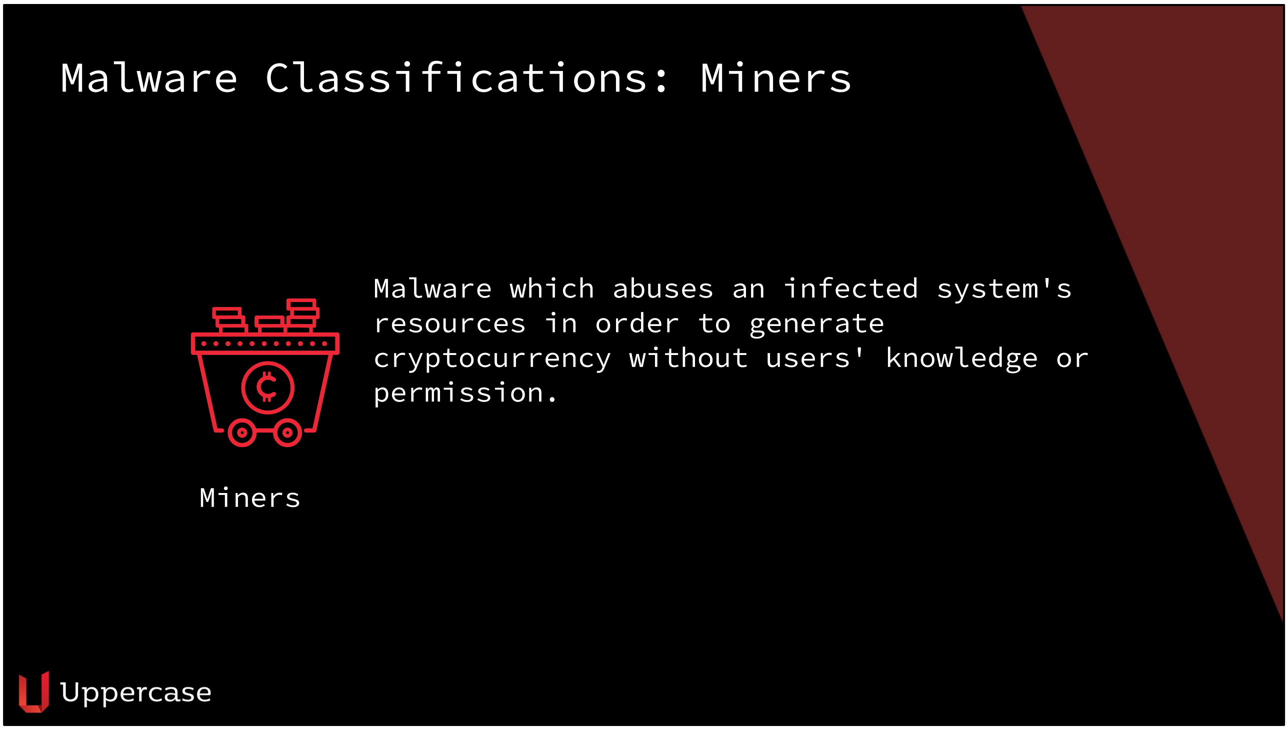
Malware Classifications: Infostealers

Malware which seeks to steal valuable data from infected systems. Typically, this type of malware often includes keyloggers as well as the capability to steal passwords which may be stored locally (especially for FTP and Email clients).

Infostealers

Uppercase

- Malware which seeks to steal valuable data from infected systems. Typically, this type of malware often includes keyloggers as well as the capability to steal passwords which may be stored locally (especially for FTP and Email clients).



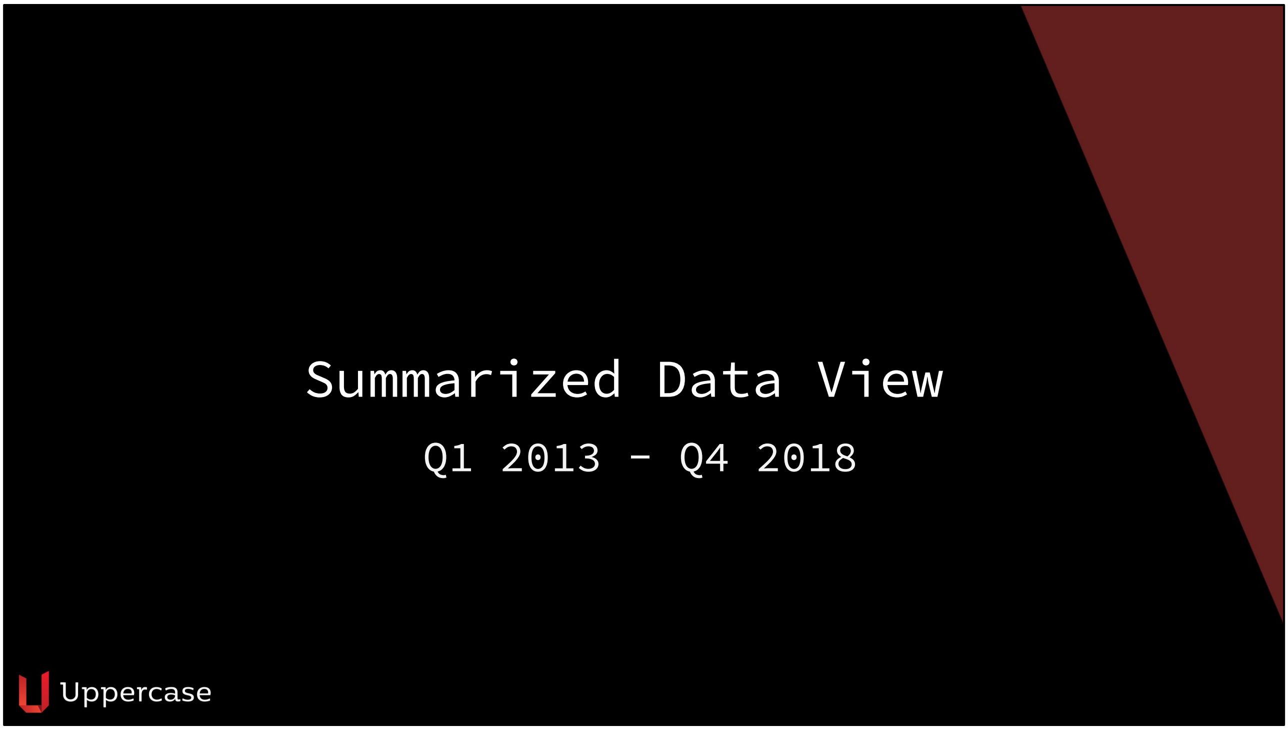
Malware Classifications: Miners

Malware which abuses an infected system's resources in order to generate cryptocurrency without users' knowledge or permission.

Miners

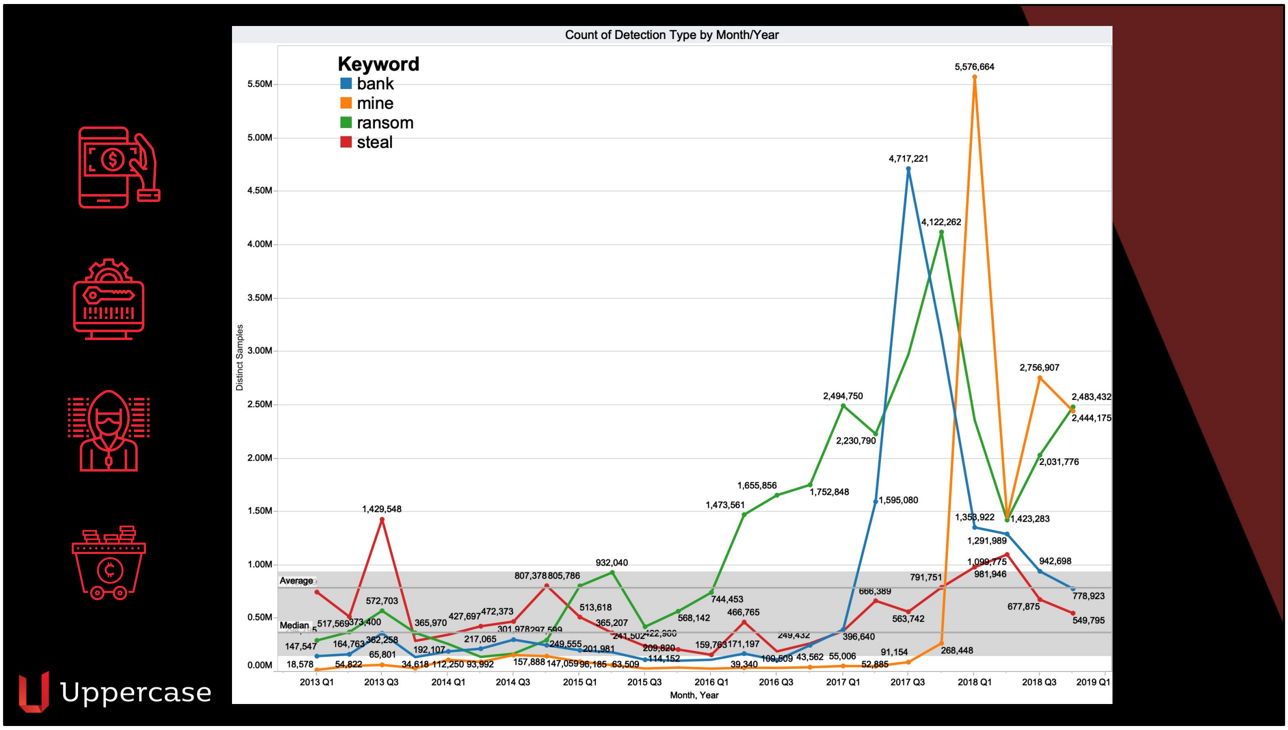
Uppercase

- Malware which abuses an infected system's resources in order to generate cryptocurrency without users' knowledge or permission.



Summarized Data View

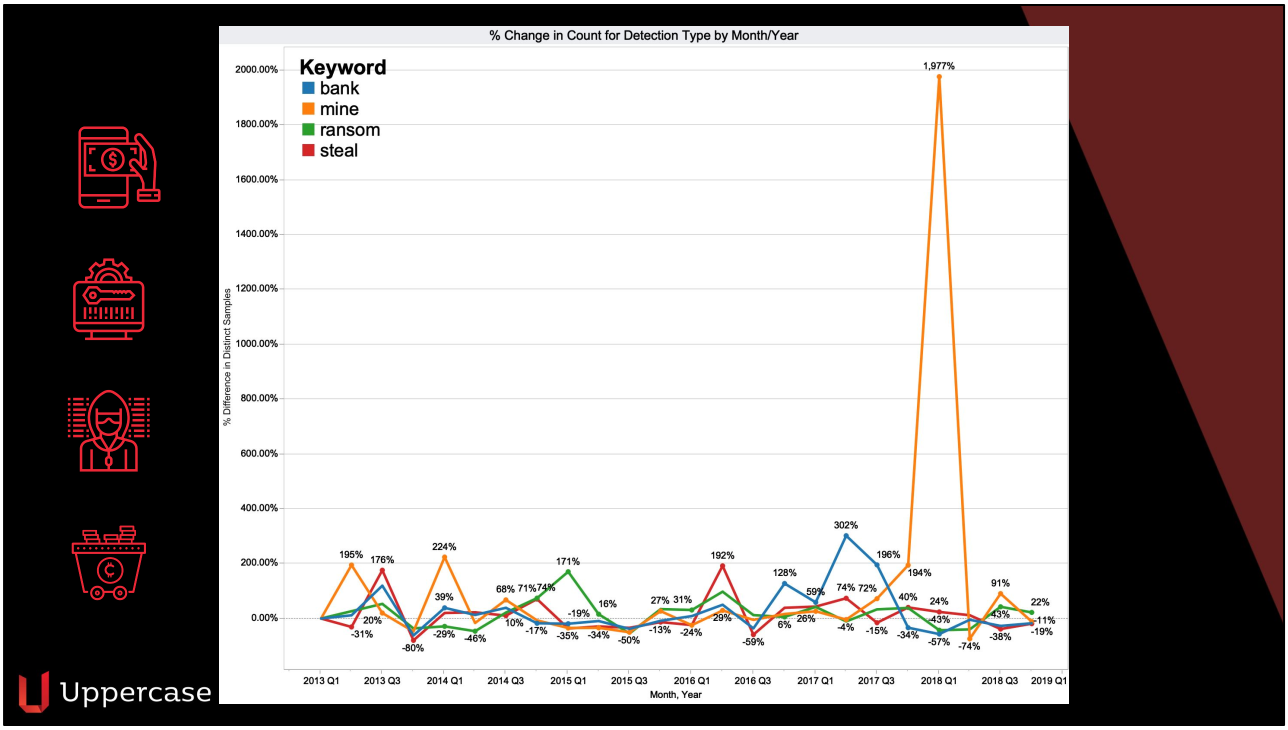
Q1 2013 - Q4 2018



The first chart presents counts of each of the 4 color-coded malware classifications based on detection type over time. You’ll notice an obvious and statistically significant increase in all four types of crimeware, especially in 2017 and 2018.

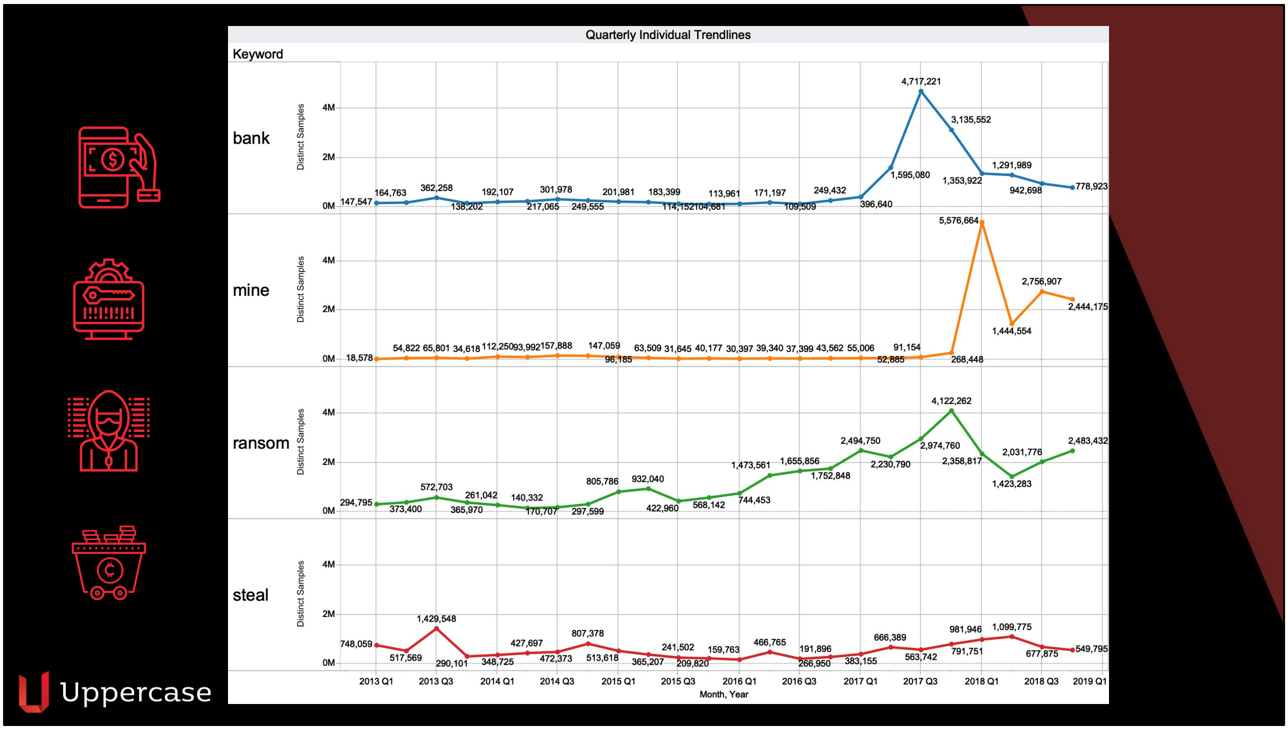
Overall line chart which shows 2013 Q1 - 2018 Q4 trends, with each point labelled. We see notable levels of growth across all measured categories.

Overall line chart which shows 2013 Q1 - 2018 Q4 trends, with each point labelled. We see notable levels of growth across all measured categories.



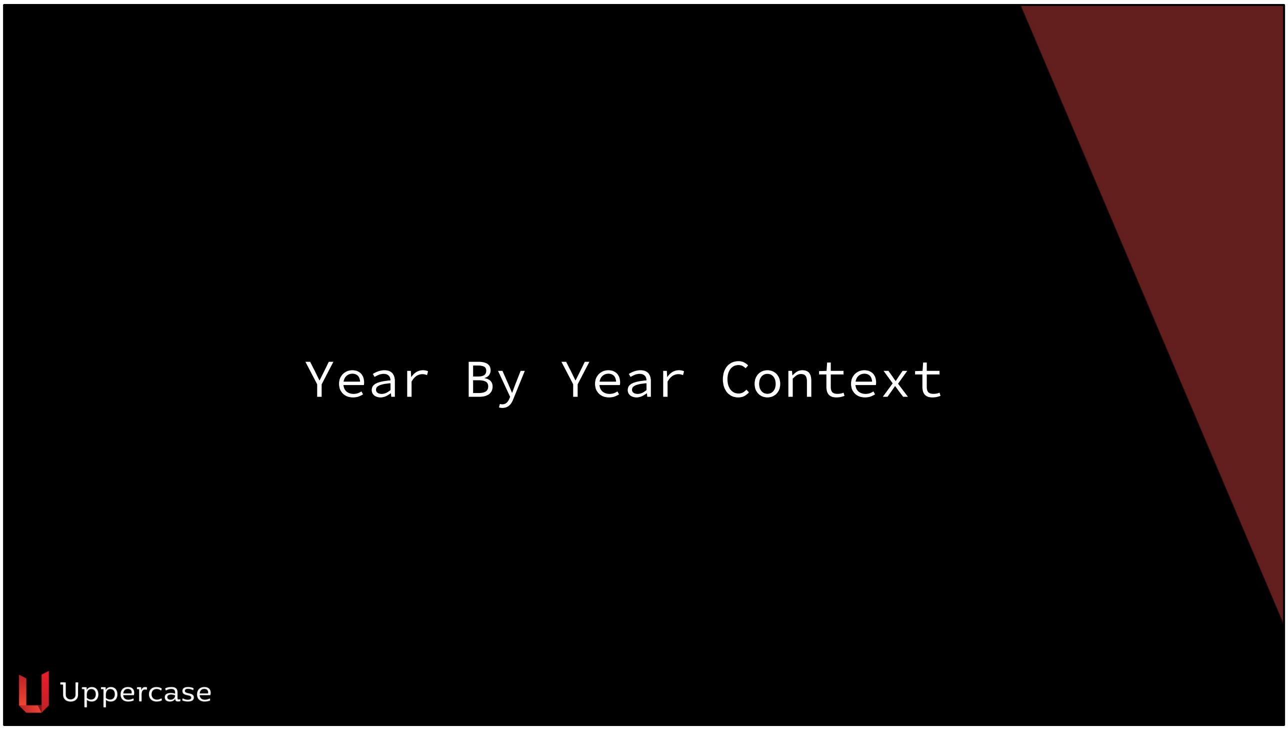
The second chart shows the quarter over quarter percentage change for each color-coded crimeware category. The incredible growth of mining malware can be seen with the enormous spike in 2018 Q1. Overall growth patterns outpace periods of decline.

Percentage changes from quarter to quarter for each malware category. In general, growth peaks far exceed valleys in terms of amplitude.



Breaking out each malware category into its own sub-graphs allows us to quickly visualize the individual trajectories of each malware label. As time has progressed we see distinct samples generally growing across the board, particularly in the later half of 2016. While infostealers did not exhibit as much growth they remained well above pre-2017 levels.

Quarterly Individual Trend lines which display 2013 Q1 - 2018 Q4 trends broken out by keyword.



Year By Year Context

Year By Year Context

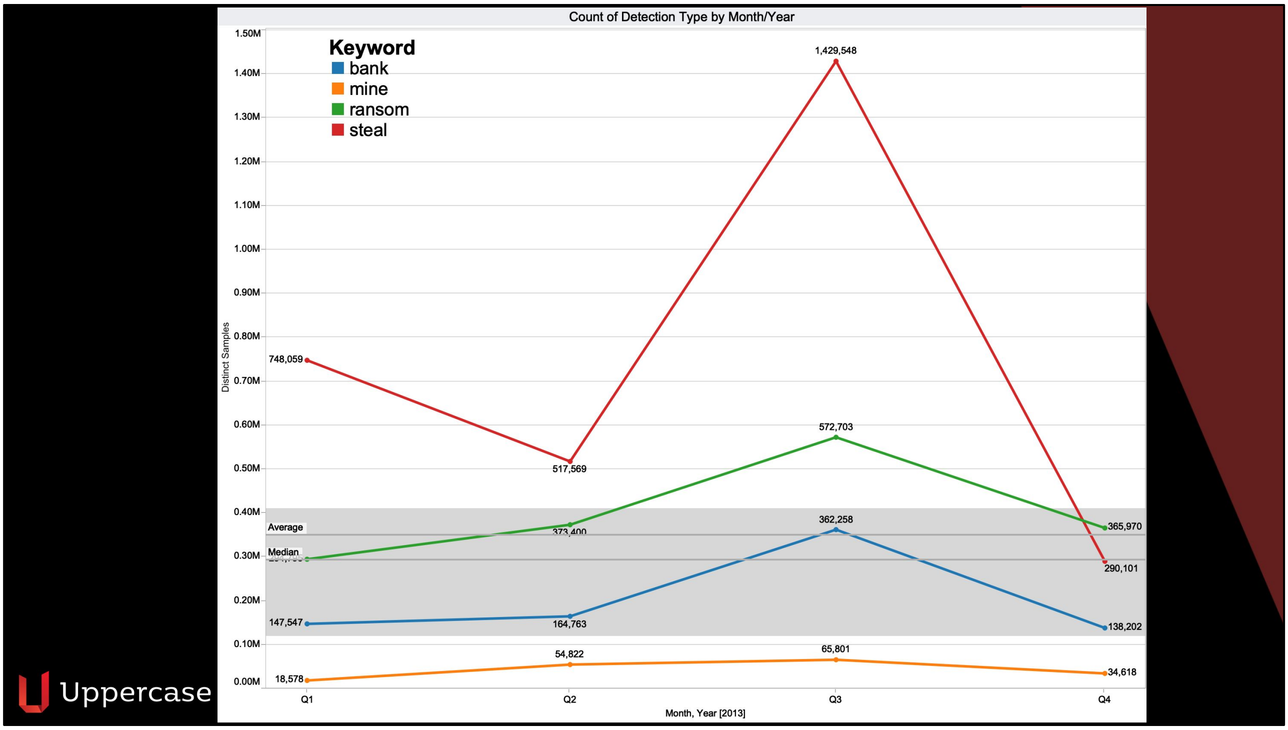
2013

Uppercase

Lead In:

2013 started off with a bang when the U.S. Department of Justice announced the arrests of the creators and distributors of the prolific banking trojan, Gozi. Unfortunately, the arrests were too little too late, as a leak of the source code lead to future Gozi adaptations and modified versions for years to come. We continue to see variants of this malware family, most commonly Ursnif, persist through 2019.

- One of the most dangerous and most rapidly proliferated techniques, specifically targeting the Google Chrome browser, rose to prominence during this time
- During this time period, malware accounted for 40% of breaches according to the 2013 Verizon Data Breach Investigations Report (DBIR). Furthermore, 75% of that 40% was the result of information stealers like keyloggers



Lead In:

2013 started off with a bang when the U.S. Department of Justice announced the arrests of the creators and distributors of the prolific banking trojan, Gozi. Unfortunately, the arrests were too little too late, as a leak of the source code lead to future Gozi adaptations and modified versions for years to come. We continue to see variants of this malware family, most commonly Ursnif, persist through 2019.

- One of the most dangerous and most rapidly proliferated techniques, specifically targeting the Google Chrome browser, rose to prominence during this time
- During this time period, malware accounted for 40% of breaches according to the 2013 Verizon Data Breach Investigations Report (DBIR). Furthermore, 75% of that 40% was the result of information stealers like keyloggers

About the Spike in Q3:
In Q3 of 2013 we observed the highest number of detections across all measured categories of crimeware. On the one hand, this is especially interesting because -- up until October 2013 -- the Blackhole Exploit Kit was infamous for proliferating malware. When its author, Paunch, was arrested during the 3rd quarter of 2013, the Blackhole Exploit kit was finally shut down. Therefore, where we expected to see a decrease in

crimeware, we saw the highest number of detections instead.

Bankers [Blue Line]

- **Citadel**, began interacting with the Chrome browser in order to Man-in-the-Browser (MiTB) encrypted banking traffic.
    - taken down in “Operation b54” in a joint effort by Microsoft’s Digital Crimes Unit, Europol’s European Cybercrime Centre (EC3), and the U.S. Federal Bureau of Investigation (FBI)
- Citadel takedown => rise of the far more dangerous P2PZeus, aka “**GameOver Zeus**.”
    - GameOver Zeus malware dates its origins back to mid-2011, it was not until Citadel was taken down that GameOver Zeus began to proliferate

Miners [Yellow Line]

- miners became more prevalent in Q1 of 2013 and continued to grow
- miners focused on Bitcoin
- not uncommon for information stealers to target Bitcoin wallets while malware miners on the same machine continued to chug away

Ransomware [Green Line]

- Did not really catch on until Q3
- The most common mechanism for spreading ransomware relied upon dropping an additional malware payload onto machines which were already infected
- most common Ransomware, **Cryptolocker**, was actually a payload installed on computers infected by GameOver Zeus

Stealers [Red]

- We assess that it is likely that **ZeroAccess** may be responsible for the spike in malware classified as “steal” in Q3
    - spike is followed by a massive falloff in Q4 => takedowns of infra by Symantec + Microsoft
- **Pony** Downloader trojan, the dropper commonly used to download Gameover Zeus, may also have contributed to the high rate of “steal” categorized malware overall

Takedowns:
Citadel:

- Q2 - taken down in “Operation b54” in a joint effort by Microsoft’s Digital Crimes Unit, Europol’s European Cybercrime Centre (EC3), and the U.S.

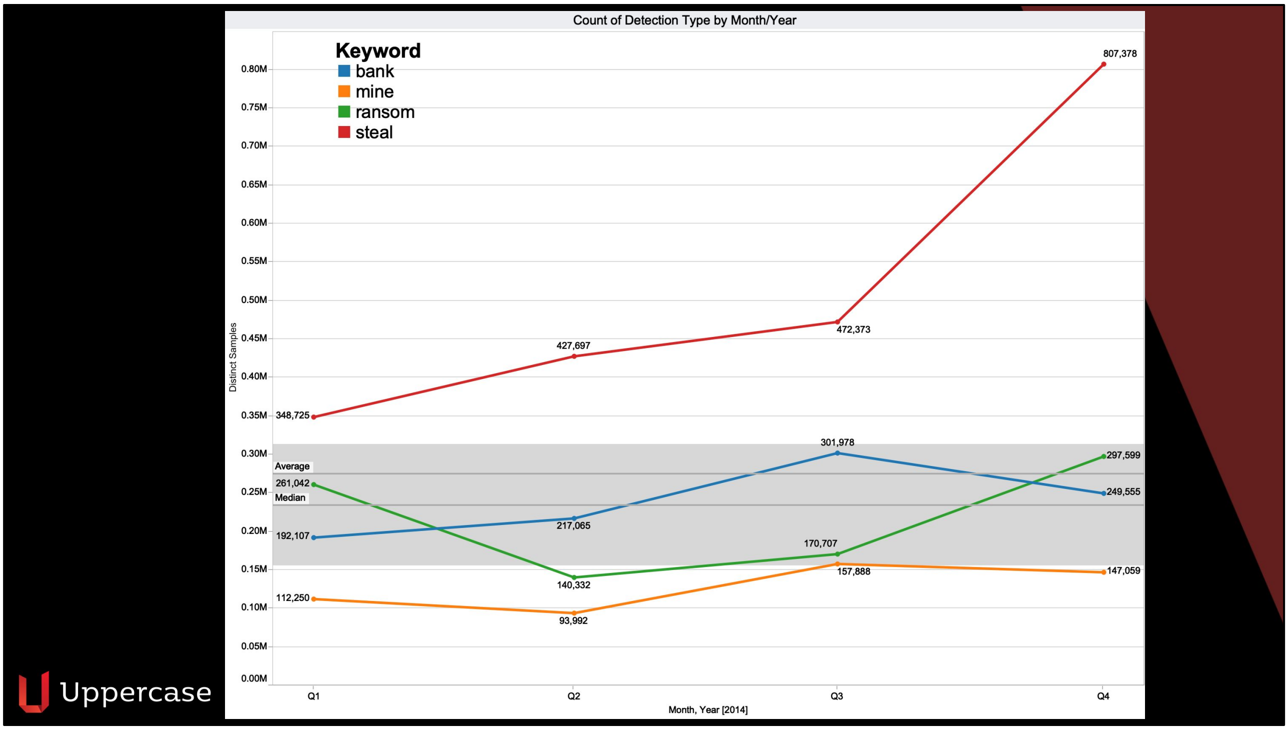
- Federal Bureau of Investigation (FBI)
- Q3 ZeroAccess - Sinkholing Began in Q3, takedown Q4

Year By Year Context

2014

Uppercase

Following a very active 2013, 2014 was relatively calm by comparison. Leaked source code for the resilient banking trojan Carberp made information security researchers expect impersonators and improvements. Although some new malware built from this leak did surface, none of the copy-cats or new impersonators ever gained the prominence of the original.



Lead In:
Following a very active 2013, 2014 was relatively calm by comparison. Leaked source code for the resilient banking trojan Carberp made information security researchers expect impersonators and improvements. Although some new malware built from this leak did surface, none of the copy-cats or new impersonators ever gained the prominence of the original.
2014 is perhaps most notable for the takedown of the GameOver Zeus botnet and its affiliates in June of 2014 as part of “Operation Tovar.” An ancillary effect of the GameOver Zeus takedown was the removal of the affiliate market for paid installs of Cryptolocker, which had been the most prolific ransomware to date

Bankers [Blue Line]

- banking trojans **Vawtrak** (Snifula/Neverquest) and **Cridex (bugatv4)** were active
- two most common banking trojans throughout 2014 were **Zeus Derivatives** and **Dyre**
  - Zeus Derivatives - variants such as **KINS** aka “**VMZeus**” and **ICE IX** quickly surfaced and made additional improvements on the original code that was leaked in 2011
  - **Dyre** took the information security world by storm shortly after the takedown of **Gameover Zeus**

        - Dyre made use of the same style of distribution by employing the **Upatre** malware. Unlike **Pony**, however, **Upatre** was streamlined to act as a downloader trojan and boasted no other capabilities other than payload drop statistics and basic host information fingerprinting

Miners [Yellow Line]

- Kaspersky stated that up to 14% of malware attacks were Bitcoin miners
- McAfee goes on to state that “The difficulty level of common mining algorithms and the nonspecialized hardware that the malware infects make this a futile effort.”
- Again: Bitcoin the sole focus

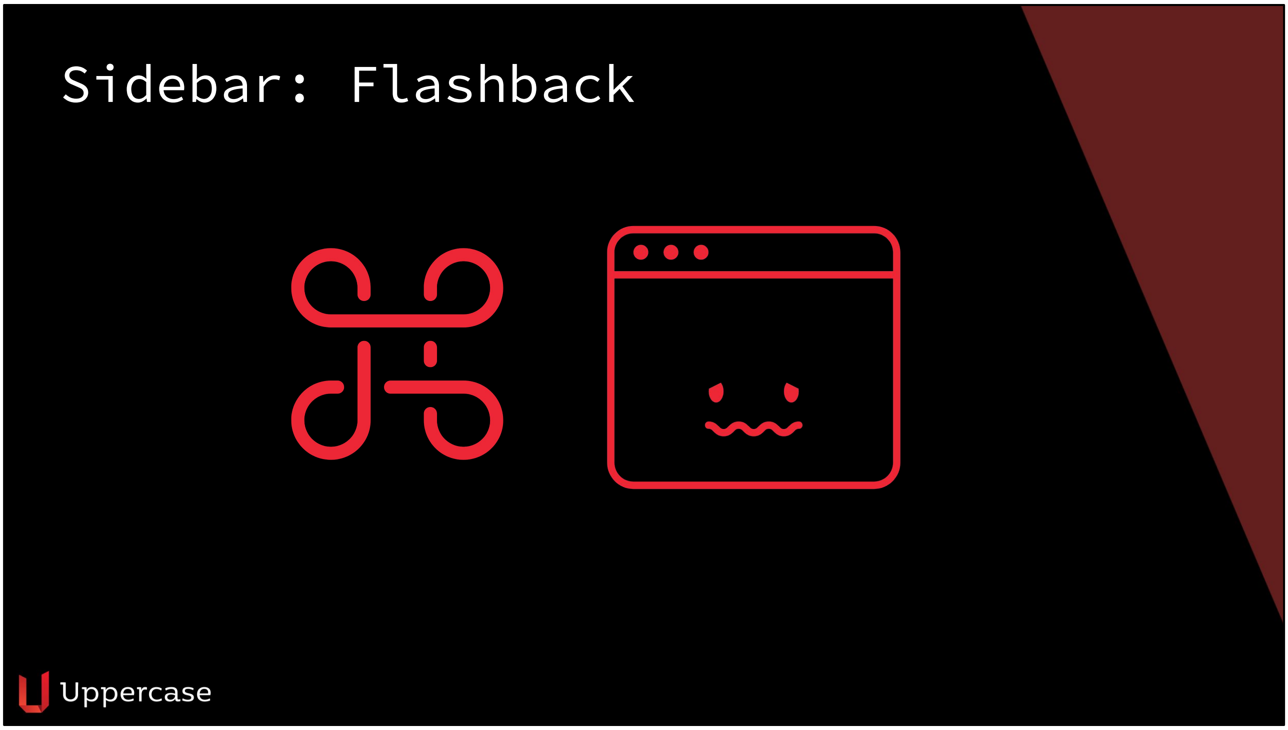
Ransomware [Green Line]

- fall of **Cryptolocker** => the variety of ransomware families surged in 2014
- Families such as **Shade (trolodesh)**, **TorrentLocker**, and **CTB-Locker** were particularly prominent.
- these families pale in comparison to the juggernaut of **Cryptowall**
    - estimated to account for **58%** of ransomware infections during this time period
- During this time period, ransomware moved from a follow on payload to a primary one and was seen distributed from exploit kits and malspam

Stealers [Red]

- Information stealing malware continued to be prevalent throughout 2014, reaching its apex right in time for the holiday season in Q4
- Notable examples of highly active malware during this time period include **BetaBot (Neuvert)**, **Kelihos**, **Cutwail**, and **Necurs**
    - In the case of Kelihos, Necurs, and Cutwail, the primary purpose of these families was spam
    - These families were responsible for, on average, over a million spam messages per day, ranging from basic pharmaceutical spam up to messages with malicious attachments and links
    - When “rented” to deliver malicious messages, the overwhelming number of emails included weaponized Office documents, a trend which would see a sharp increase in the years to come

Takedowns:
GOZ:
Q2 - GameOver Zeus botnet and its affiliates in Q2 - June of 2014 as part of “Operation Tovar.



Sidebar: Flashback

Uppercase

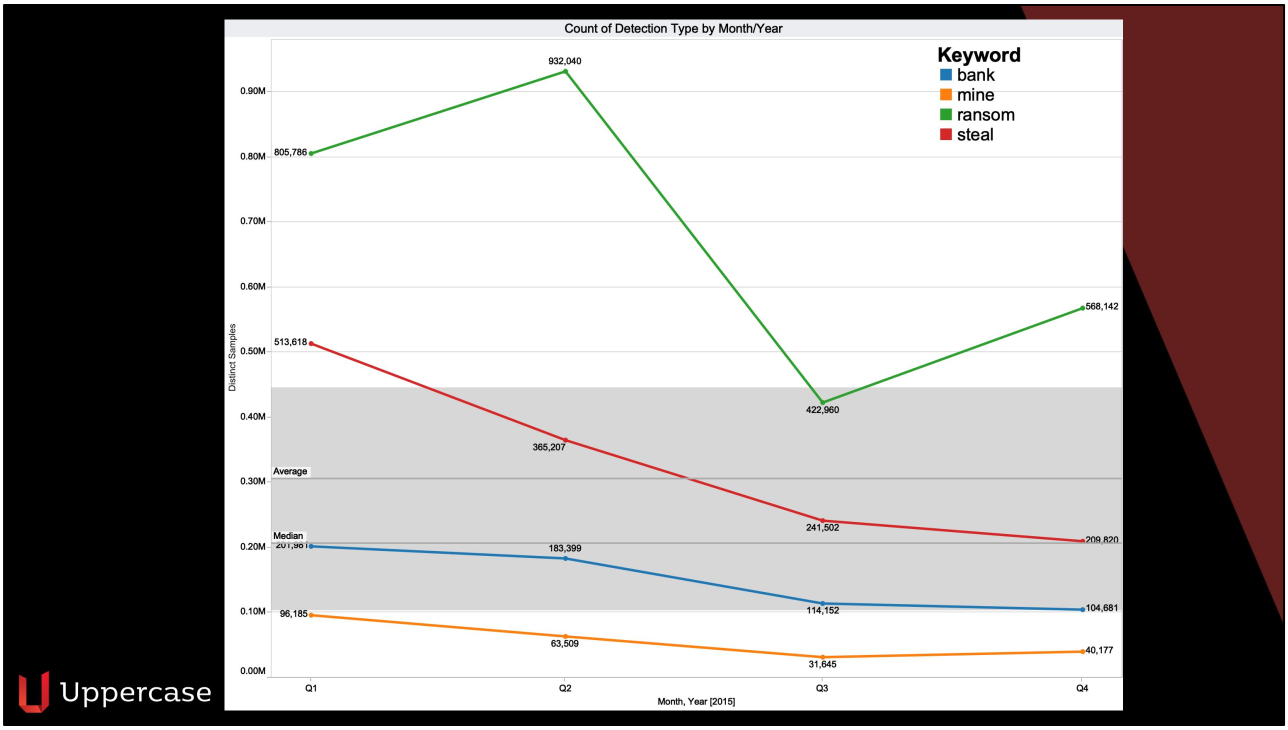
A quick aside: for the most part during this analysis, we've focused solely on malware affecting Windows hosts, but 2014 saw the largest (to date) infection of OSX systems with a variant of the Flashback click fraud malware. A reported 600,000 OSX devices were infected in 2014 after an unpatched vulnerability in Oracle's Java led to the installation of a fake Adobe Flashplayer installer. While this particular variant of malware doesn't really fall into any of the broad categories we used for assessing malware trends, this author feels it is important to detail this pivotal event in the history of OSX malware.

Year By Year Context

2015

Uppercase

The legal actions taken against prominent criminal threats in 2014 led to the subsequent rise of two new banking threats: Dridex and Dyre. The years to come additionally brought a sharp rise in unique ransomware strains as malware authors diversified their financially-motivated repertoires. Threat actors responded to threats against their livelihoods in much the same way as the greek legend of the hydra: cut off one head and an exponentially increasing number appeared.



Lead In:
2015 picked up right where 2014 left off with a continued upward trend in ransomware, which far outpaced the growth of all other studied malware categories. 2015 saw an overall decline in distinct samples of bankers, miners, and stealers. While at first glance this may indicate an overall shrinkage of in-the-wild samples of malware that falls within those categories, the reality is a bit murkier.

Bankers [Blue Line]

- Consolidation and affiliate services, aka “crimeware as a service,” came to the forefront during 2015
  - **Dyre**
  - **Dridex**
  - The business models of both families of malware allowed actors to buy everything they needed in an “off-the-shelf” manner, relying on the seller to provide infrastructure, control panels, and malware
  - shifting into **service-based business models streamlined deployment** and i**ncreased reliability** of management => the overall downward trend in prevalence for bankers
- Smaller, region-specific banker families such as **Shiotob** and **Tinba** continued to hold steady in general prevalence.

Miners [Yellow Line]

- interest piqued in 2014, threat actors seemed to be moving all in on ransomware as the most streamlined monetization option
- shift of focus from bankers to ransomware in 2015, miners remained relatively uncommon
- primarily focused on Bitcoin
- diametrically opposed strategies combined with the growing effectiveness of the threat of data loss from ransomware caused miners to stay fairly quiet throughout 2015

Ransomware [Green Line]

- Though “traditional” models of monetizing compromised hosts (such as bank account manipulation or credential theft) appeared to be falling out of favor, ransomware saw a boom in growth in both unique families and distribution throughout 2015
  - In a 2015 study of ransomware, Symantec reported that 11 of the top 12 countries impacted by ransomware fell within the G20.
- The number of encryptor variants of ransomware had skyrocketed in 2015
  - **CryptoWall** accounted for more than **58%** of observed ransomware infections during the **first half of the year**
  - By the end of 2015 (and into 2016), **TeslaCrypt** had overtaken **CryptoWall**, accounting for **48%** of observed ransomware compromises
- Kaspersky reports the most prolific threats, **CryptoWall, Cryakl, Scatter, Mor, CTB-Locker, Torrent-Locker, Fury, Lortok, Aura, and Shade**, “...were able to attack **101,568** users around the world, accounting for **77.48%** of all users attacked with crypto-ransomware during the period.”
- New techniques were also pioneered during this era, as Symantec indicates that attackers using crypto-ransomware were setting d**ynamic pricing based on victim location**

Stealers [Red]

- Pony Downloader Trojan’s code leakage, possibly prompted by a sale, caused a marked increase in the availability of highly reliable malware
  - the newer version, 2.0, had massively increased capabilities focused on information stealing both from a local host and from the web browser.

Takedowns:
Ramnit

Q1 -The first major takedown occurred in February of 2015 with the seizure of infrastructure belonging to the operators of Ramnit. Only partially successful.

Simda
Q2 - April of 2015 saw the takedown of of the SIMDA botnet; a notorious infostealer first observed in 2009. This takedown was a joint effort by the US DHS and Interpol and impacted more than 700,000 hosts

Dridex
Q4 - Dridex (bugat v5) which coincided with the takeover of the botnet. Dridex had seen an increase in popularity throughout 2015, mostly impacting the US, Japan, and Germany. This takedown was only partially effective and by mid-2016 Dridex would come roaring back in force.

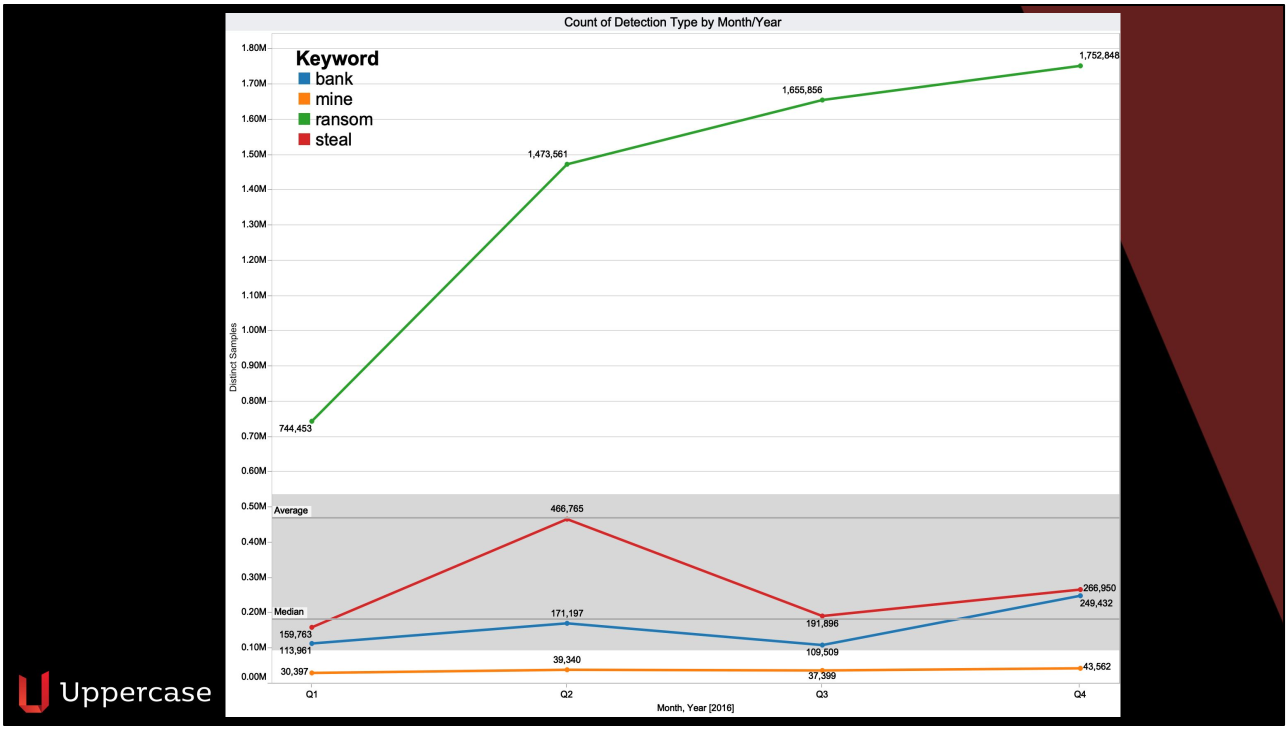
Dyre
Q4 - in November, several operators of the Dyre banking trojan were arrested in a raid on a Moscow office. Shortly thereafter, Dyre campaigns and operations ceased entirely.

Year By Year Context

2016

Uppercase

Hot on the tail of 2015, 2016 brought about a true explosion of ransomware crypto variants. Similarly to 2015, other than a quick spike of infostealers in Q2, we see a general decrease throughout most of the year across all other crimeware categories.



Lead In:
Similarly to 2015, other than a quick spike of infostealers in Q2, we see a general decrease throughout most of the year across all other crimeware categories. The general thread of aggressive monetization through extortion continued to gain momentum with no signs of slowing down. This is a fascinating change that sees malicious actors interacting more frequently with their victims. Europol states in their 2015 IOCTA,

> "Whilst the cautious, stealthy approach goes with the stereotype of the uncertain, geeky hacker, the aggressive, confrontational approach of putting blunt pressure on individuals and businesses bears the signature of organized crime."

This assessment is supported by the massive increase in both ransomware infections and unique ransomware families throughout 2016. Organization of services and support apparatus were the key enablers: this manifests itself as both Crimeware as a Service (CaaS) and Ransomware as a Service (RaaS) and was highlighted as part of the consolidation of malware services that began in 2015.

Lead In 2 Corporate Victims:
As 2015 closed, researchers observed that **corporate systems were an increasing**

percentage of crimeware victims.

ESET: “We can see that the barrier separating general purpose malware from directed attacks is becoming more transparent.” In other words, the impact of crimeware on businesses of all sizes had begun rapidly catching up to more targeted types of attacks.
Kaspersky: In their 2014-2016 ransomware review that corporate users attacked with ransomware increased nearly 6x from 2014-2015.

Bankers [Blue Line]

- The popularity of banking malware continued to wane in the face of the continued success of ransomware.
- the most common banker in 2016 was a malware family thought to have gone extinct: **Ramnit**
- According to Symantec, the Japanese regionally targeted **Bebloh** banking trojan was a close second
- Rounding out the top 5 are the ever-present **Zeus derivatives (PandaZeus**), **Neverquest** (aka **Vawtrak**), and **Dridex**
- Compromises involving multiple types of crimeware slowly became more prevalent, as was the case for traditional banking malware **Dridex** following the **GameOver Zeus** model of dropping the **Cerber** ransomware post infection
- According to Kaspersky, Mobile (Android) banking trojans made up nearly a third of all banking Trojan detections

Miners [Yellow Line]

- Recognizing cryptocurrencies as legitimate opportunities for increased monetization, threat actors iterated on their infostealers and bankers to steal cryptocurrency **wallets**. **Dridex** implemented this change in September of 2016. Despite the increased attention given to cryptocurrency, cryptominers remained uncommon

Ransomware [Green Line]

- first half of 2016 was dominated by the **TeslaCrypt** ransomware
    - **TeslaCrypt** was distributed either from various exploit kits (**Angler EK**, **Neutrino EK**, **Sweet Orange EK**, **Nuclear EK**) r as a malspam payload from **Nemucod**
    - This diversity of distribution methods led to its dominance over all other variants of ransomware until March of 2016 when the operators behind **TeslaCrypt** released the master decryption key and announced their retirement.
- Up and comers **Locky** and **Cerber** quickly filled in the absence

    - The **Locky** family is a particularly interesting case as it utilized the same **distribution mechanisms** (**Necurs**) as the **Dridex** botnet and often ran mutually exclusive to **Dridex** Campaigns

Stealers [Red]

- 2016 was a banner year for the Necurs botnet operators who were the primary spammers (i.e., the delivery mechanism) behind Locky, Cerber, Dridex, and Kovter.
- as a service" applied to cybercrime
- "malspam for hire" botnet was primarily used by various affiliates of the aforementioned malware in massive campaigns delivering malicious office documents, javascript, or other scripting language to facilitate the download of the desired payload

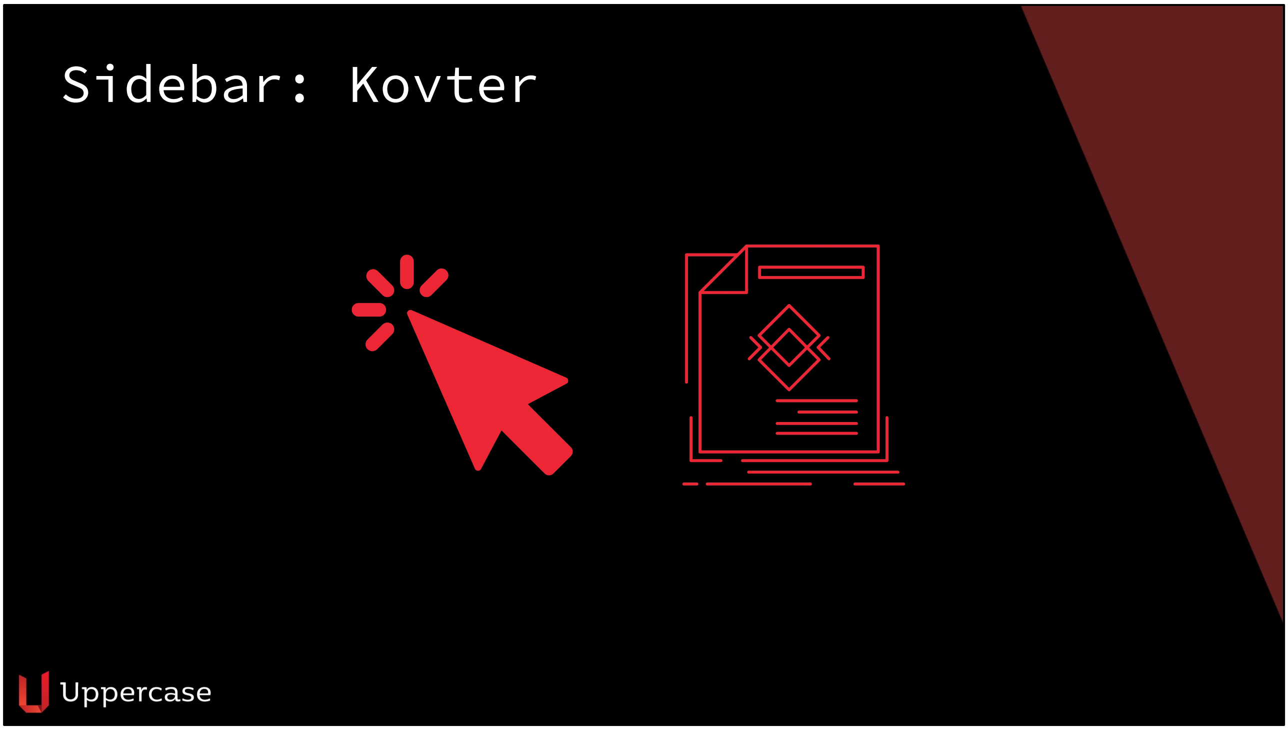
Takedowns

Q2 - Lurk - Russian authorities arrested the members of the "Lurk" group which had targeted Russian financial institutions since 2011.

- These arrests happen to coincide with the disappearance of the Angler Exploit Kit, which eventually led to the revelation that the group were the exploit kits' operators

Q4 - Avalanche - resulted in the arrests of 5 individuals, the seizure of 39 servers, and the offlining of 221 additional servers

- This resulted in the disruption of multiple crimeware families, including Nymaim, Corebot, URLzone, NeverQuest, and more



Sidebar: Kovter

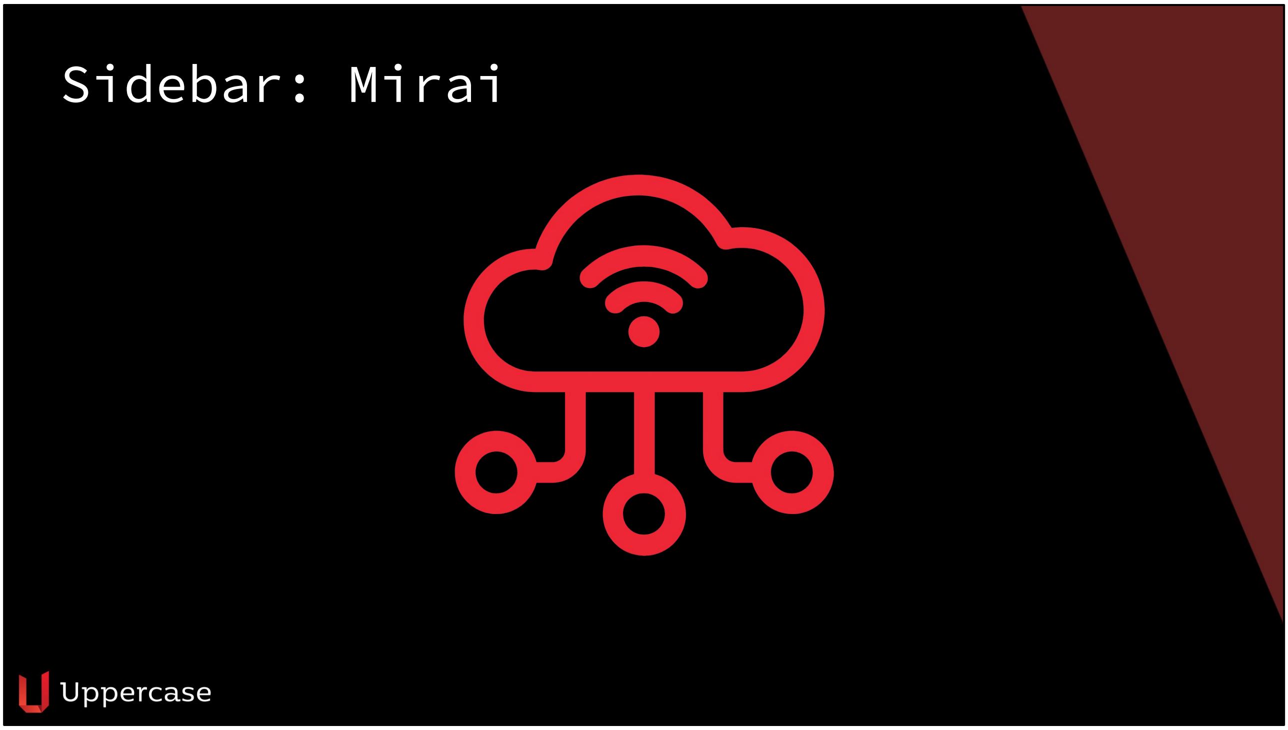
Uppercase

One of the stranger evolutions of malware during this time period can be seen in the Kovter family. Kovter began its life as ransomware, purporting to be software from law enforcement cracking down on illegal file sharing and demanding a ransom. A second variant of Kovter focused on ad fraud. In 2015, Kovter became one of the most notable “fileless” malware families and in 2016 it had further refined its registry persistence techniques. While Kovter was a significant player during 2016, as evidenced by its widespread distribution from both malspam and exploit kits, it is not specifically included in the evaluation of crimeware trends. This is due to its primary functionality as an ad fraud engine. This technique doesn’t neatly fall within any of the outlined categories, though it may most closely fit in with miners as it is abuse of a computer’s resources. That said, we believe Kovter deserves special attention as a malware family that paved the way for future fileless malware techniques and unique mechanisms for monetization at scale.

Sidebar: SWIFT Attacks

SWIFT
Uppercase

2016 was also a breakout year for attacks against the SWIFT messaging system which facilitates interbank communications. In April, more than 81 million dollars were stolen from a financial institution in Bangladesh by state nexus threat actors. These threat actors deployed malware which modified SWIFT messages to bypass transaction validity checks. Several months later, Fin7 was seen using small executables to suppress records of SWIFT messages. These examples illustrate the increasing sophistication of threat actors with financial motivations.



Sidebar: Mirai

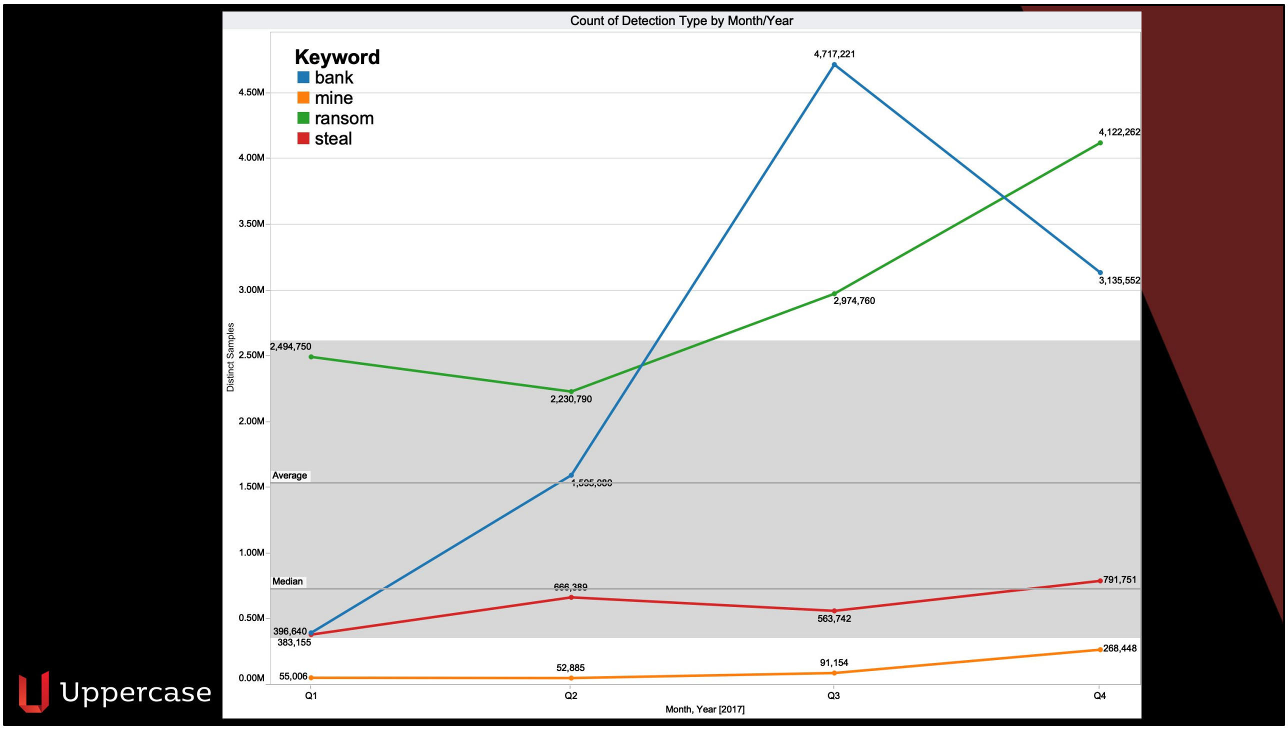
Uppercase

Perhaps the most pivotal malware-related event of 2016 has little to do with traditional crimeware. Mirai, a family of malware targeting linux based “internet of things” (IoT) devices, made an enormous splash in September of 2016 when popular investigative journalist Brian Krebs's website was taken offline with a 620 Gbit/s distributed denial of service (DDoS) attack. This was quickly followed up by a 1 Tbit/s attack on the web host, OVH. These attacks continued throughout the remainder of 2016 with additional high profile service Dyn being targeted by a DDoS attack as well. At its peak, Mirai would enlist roughly 600,000 vulnerable IoT devices including cameras, routers, and other internet connected consumer goods. While this doesn’t fall within any of the outlined categories of crimeware, it is important to note that IoT was finally thrust into the spotlight due to Mirai. In the coming years, we will see a shift from DDoS bots to cryptominers on these devices.

Year By Year Context

2017

Uppercase



Lead In:
2017 was the year of opportunity for crimeware authors. Ransomware began to crowd itself out of the market, yet new exploits allowed for wormable, destructive variants. Emotet, a dated banking trojan, would experience a renaissance and a cryptocurrency rush would fuel an 8,500% increase in mining malware deployed on victim machines. This surge in malware activity is noted by Europol in their 2017 IOCTA in which they state, “A handful of cyber-attacks have caused wide-spread public concern but only represented a small sample of the wide array of cyber threats now faced.” Ultimately, changes in the threat landscape caused major headaches for defenders across the globe.

Bankers [Blue Line]

- The overall downward trend in bankers observed over the past 3 years sharply overcorrected with the resurgence of **Emotet** in March of 2017 and the expansion of **Dridex** malspam campaigns
- The first half of the year was dominated by **Dridex** campaigns. **Dridex** continued to evolve, with a new version targeting victims across Europe
  - Analysis of the loader used in this new version of **Dridex** caused Kaspersky to speculate that the same group using **Dridex** may have also been behind **GameOver Zeus**

- **Emotet** eschewed exploit kits in favor of massive email campaigns which ran from Monday to Friday of each week, with spikes in activity beginning in March with a peak growth of over **2,000%** by Q4 of 2017
- **Dridex** and **Emotet** made the biggest splashes, **Ramnit**, **Tinba**, and **Zeus Variants** continued to see popularity
- **Trickbot**, a likely derivative of **Dyre (operationally)**, began propagating via malspam by the middle of 2017 (though it would not peak until 2018), thus rounding out the top global banking threats

Miners [Yellow Line]

- Miners stayed flat UNTIL: massive spike in cryptocurrency values towards the later half of Q4 2017
    - "coinminers" (miners) gained massive popularity amongst threat actors seeking to take advantage of the explosion in cryptocurrency valuations
    - Miners of this era fall into two categories: **file-based**, which requires the execution of a miner on a victim, and **browser-based** such as coinhive, which takes place within the context of a user's browser irrespective of operating system
    - Propagation of miners spread across the spectrum of distribution channels including exploit kits, malspam, drive-by mining code, and 3rd party bundlers
    - Mining falls on the opposite spectrum of the ransomware attacks that it supplanted: while ransomware is overt and attention grabbing, miners must remain stealthy for as long as possible to derive profits
    - Symantec estimates total growth in coinmining activity (including browser-based or drive-by schemes) at around 34,000% in the final quarter of 2017 (mostly attributed to browser based miners)

Ransomware [Green Line]

- Symantec speculates the explosion of ransomware in 2016 caused a market retraction in 2017 which resulted in a decrease in ransomware families and lower ransom demands
- The beginning of the year saw a new offline ransomware called **Sage**, which used a variety of distribution methods, including the **RIG Exploit Kit** and multiple spamming botnets,
- Following its apparent fall from grace, **Locky** was seemingly replaced with **Jaff** in May of 2017 and once again made use of the **Dridex-esqe** malspam channels of its predecessor
- Another new family to rise to fame was **GlobeImposter**, which was fueled by

- enormous malspam campaigns and may have been used by a particular **Dridex** affiliate
- A new player on the scene, **Spora**, offered offline encryption requiring no network communications as part of their core offering of "ransomware-as-a-service" and met some success by advertising on criminal web forums

Destructive "Ransomware"

- WannaCry
  - Unlikely to have been financially motivated, doomsday came to the internet in May of 2017 with the release of **WannaCry**
  - **WannaCry** particularly dangerous was the inclusion of **EternalBlue** (MS17-010)
    - SMB exploit allowed WannaCry to spread like wildfire on internal networks and across the internet at large
  - Due to the trivial ease with which payment addresses can be manipulated in the malware, hundreds of thousands of copy-cat WannaCry samples continue to infect vulnerable users to this day
  - WannaCry dominated headlines from all major international news outlets for weeks, which eventually led to attribution and blame being pointed at North Korea
- NotPetya
  - Originally targeted Ukraine via MeDoc (national tax software)
  - Utilized the **EternalBlue** exploit but additionally included another SMB exploit from the Shadow Brokers called **EternalRomance**
  - Particularly destructive because it rendered infected hosts unusable by overwriting critical sectors of the hard drives' boot sectors
  - Quickly spread beyond Ukraine due to the effectiveness of its SMB worm mechanisms
  - Collateral damage outside of Ukraine included FedEx and Maersk, with the net total damages nearing $10 billion, a cost nearly **one thousand times greater** than that of WannaCry.

Stealers [Red]

- Ursnif/Gozi stayed popular as the most frequently seen infostealer
- Andromeda was also fairly prevelant
- Not really any stand out families this year. We speculate that the rise in stealers mirrors that of bankers due to the increasing modularization of the

- later

Takedowns
Dozens of indictments targeting financially motivated threat actors indicated that law enforcement was growing more capable of executing cybercrime investigations

Neverquest/Vawtrak Q1 - Arrest of author in Spain

- Previously had distribution and hosting impacted by Avalanche in Q4 2016
- had previously been one of the top five most common bankers

Kelihos - Q2 Kelihos had survived numerous takedown attempts in the past which included one in 2011 and a coordinated sinkholing effort in 2012

- Kelihos was primarily responsible for immense amounts of spam campaigns, including Apple phishes. and pump and dump stock scams, though the malware was also associated with DDoS attacks, click fraud, bitcoin mining, and cryptocurrency wallet theft.
- Kelihos was also used in the distribution of ransomware and banking trojans

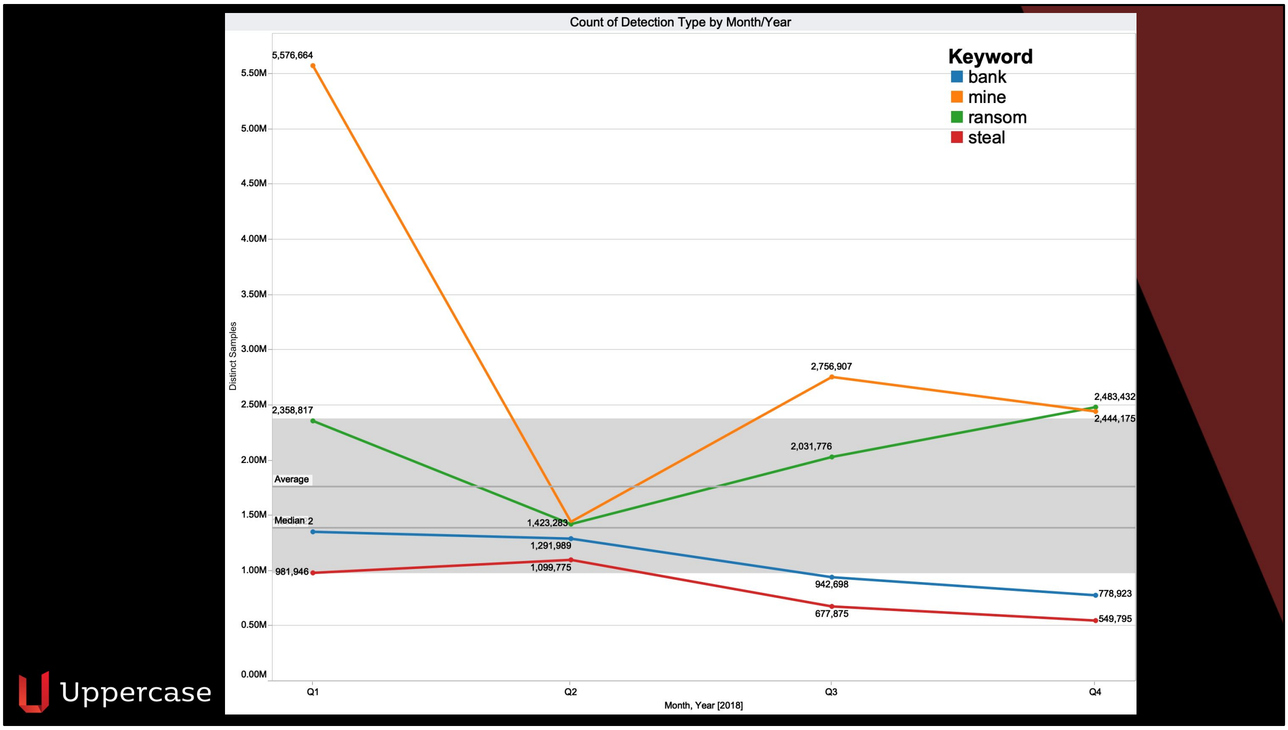
Andromeda - Q4

- Andromeda was responsible for distribution of the **Petya** and **Cerber** ransomware families and infostealers such as **Ursnif** and **Pony**.
- Despite its prevalence in Asian countries, Andromeda was a global phenomenon detected on nearly 1,000,000 machines per month in the 6 months prior to its takedown.

Year By Year Context

2018

Uppercase



Lead In:
2018 saw a continued decline in ransomware and a dramatic fall in miners, while banking trojans and infostealers remained relatively consistent in their utilization. While the first half of the year saw a diversification of mining malware, a massive crash in cryptocurrency valuations seemingly drove criminals back to the tried and true techniques of yore sprinkled with some light innovation.

Banking trojans, such as Emotet and TrickBot, blurred the boundaries between traditional banker and infostealer malware by introducing highly customizable, modular frameworks which allowed attackers to pick and choose capabilities. Finally, we saw the advent of “formjacking” (which we will categorize as an infostealer) have massive impacts on ecommerce websites

Bankers [Blue Line]

- death knell of the specialized banking trojan => 2018
    - Two of the more insidious families of banking trojan, **Trickbot** and **Emotet**, introduced new modules to expand their respective capabilities into remote access, local password theft, [crypto] wallet theft, self propagation, and spam
- Further changes in the global malware ecosystem would take place by mid-year 2018

    - **Trickbot** forewent its own malspam campaigns in favor of leveraging **Emotet** as a dropper
    - **Bokbot**, aka **IcedID**, a derivative of **NeverQuest,** was also delivered as a payload by **Emotet**
    - **Ramnit**, retained its position as one of the top financial trojans with expanded functionality focusing on overhauled web-injects
        - **Ramnit** threat actors may also have partnered with criminals utilizing the infostealer, **Azorult**
- One side effect of the malspam approach was the increasing frequency of business assets falling victim to malware whose interests were primarily consumer focused
    - These business beachheads may ultimately have caused a **shift in ransomware tactics that saw highly targeted**, manual deployments to **high-value victims**.

Miners [Yellow Line]

- The bull market run of cryptocurrencies, as best mapped by the Bitcoin Index, reached its peak at the end of 2017 and began to crash by February of 2018
    - Following this trend, cryptominer activity dropped by more than 50% over the course of the year.
- The popularity of mining malware even spread to threat actors who traditionally participated in espionage operations (Roaming Mantis), though several state nexus actors also attacked exchanges directly (Lazarus)
- While the overwhelming rush towards miners began to drop, miners were still the **most prevalent malware type of 2018**
- Browser based miners overtook exploit kits as the preeminent payload deployed to vulnerable websites
    - This is illustrated during the course of “Drupalgeddon” campaigns, which saw threat actors injecting browser based miners, such as coinhive, during Q1 and Q2 of 2018
- Coinhive’s announced shutdown coincides with the sharp decline in miner detections observed from Q2-Q3
    - Despite this shutdown, the low barrier to entry of miner malware combined with its relative stealthiness, anonymity, and cross-platform deployment (including mobile) ensured that it would remain a popular technique for cyber criminals

Ransomware [Green Line]

- RaaS
    - (RaaS) had a breakout year in 2018 with the popularity and rapid

  - iteration of **GandCrab**
    - **GandCrab** prided itself as an easy-to-use service allowing for full deployment with just a few clicks
    - could be distributed via numerous channels including exploit kits and malspam.
  - **GandCrab** would continue to dominate the commodity ransomware market until its authors announced their retirement in mid-2019

- Enterprise Targeted Ransomware
  - Enterprise ransomware **deployments were up by 12%** over the previous year while **overall ransomware detections were down by 20%**
    - Europol's OCTA - "in a few short years, ransomware has become a staple attack tool for cybercriminals, rapidly accommodating aspects common to other successful malware such as affiliate programs and as-a-service business models"
  - While overall ransomware infections fell off, **targeted, manual deployments** of ransomware took their place as exemplified by the success of **Bitpaymer, SamSam, Dharma, and Ryuk**
    - Crowdstrike codifies this particular tactic as *"big game hunting"* and has observed multiple criminal groups shifting to a more manual deployment model
    - tactical deployment not only allows for target selection, but also allows for asset selection within a target's environment
      - may include network shares or backup services
    - One of the earliest families to show success using this more direct deployment tactic was **SamSam**, which impacted 67 different organizations in 2018
      - Following the indictment of two Iranian nationals by the US DOJ, **SamSam** went relatively quiet
    - Many groups, such as the criminals behind the **Dharm**a ransomware, utilized weak **Remote Desktop Protocol (RDP)** credentials open to the internet to gain initial access
    - **Ryuk**, on the other hand, appeared to selectively target organizations who have already been compromised by **Trickbot** or **Emotet**
  - Estimates by Crowdstrike place revenues at over $10 million across 3 of the most high profile threat groups.

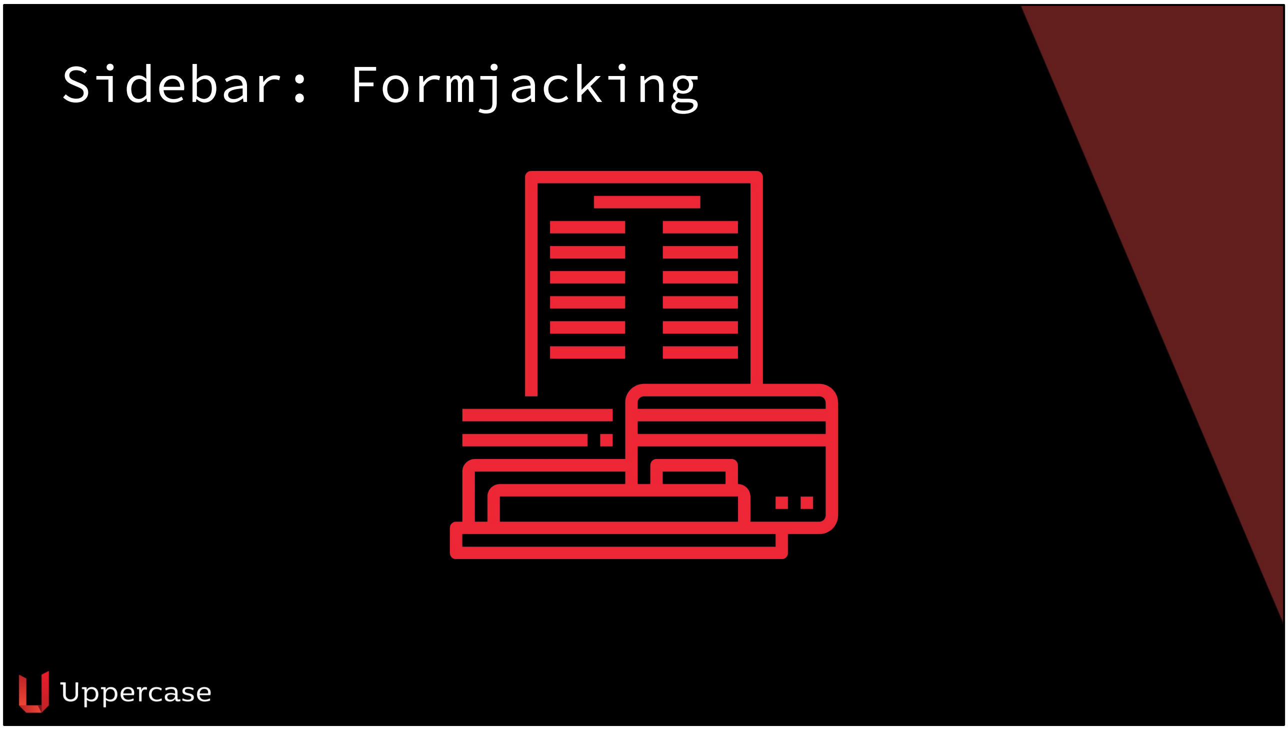
Stealers [Red]

- With the consolidation of stealer capabilities and bankers, overall bespoke

- infostealer numbers saw a decline over the course of the year. HawkEye and other Stealers remained active, but in relatively small numbers. THe majority of novel Infostealer activity falls into the Formjacking category.

Takedowns:
3ve - Q4 massive global ad fraud scheme The primary malware components of 3ve, Miuref (aka Boaxxe) and Kovter controlled more than 1.7 million IP addresses at the time of takedown

Not really a takedown - Q2 major arrests of 2018 targeted perhaps one of the most high profile “APTs” of financially motivated threat actors, Fin7, which saw three of its leaders arrested in Spain, Germany, and Poland.



Sidebar: Formjacking

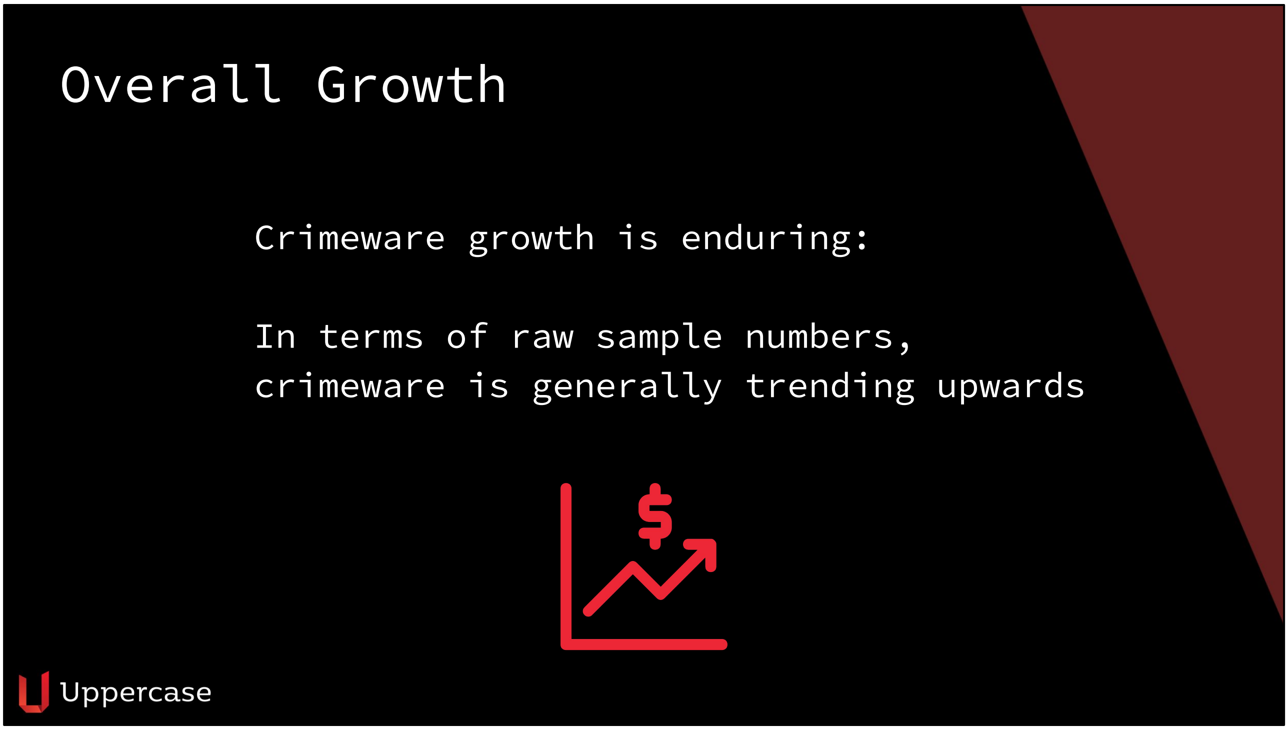
Uppercase

Payment card data has always been an opportune target for financially motivated criminals. Formjacking, the use of malicious JavaScript to steal credit card details from payment forms on ecommerce platforms, rose to prominence after headlines broke of massive breaches at British Airways, TicketMaster, and Newegg. Formjacking is effectively a browser-based infostealer, and the perpetrators of these attacks are made up of multiple groups which fall under the label “Magecart.” The 7 groups that are categorized under this umbrella label specialize in placing digital credit card skimmers, which have collectively accounted for hundreds of thousands of payment card details being stolen. Formjacking doesn’t require access to a backend database, merely the ability to breach web front ends to deploy stealthy code. With upwards of 17,000 domains compromised as of 2019, this technique shows no signs of slowing down.

Discussion

Uppercase

Crimeware has been a long-standing mainstay of the financially motivated threat actor’s toolset. The constant shifts and updates in tools and techniques, from bankers and infostealers to ransomware and miners [and back again], have resulted in a long standing game of cat and mouse between attackers and defenders. The last six years have been a roller coaster ride of consolidation and expansion, new monetization techniques, a massively increased threat landscape, and global law enforcement action against financially motivated threat actors. Now that we have explored the historical context of six years and hundreds of millions of distinct samples, lets work to interpret the data with a focus on the critical questions outlined at the beginning of this paper.



Overall Growth

Crimeware growth is enduring:

In terms of raw sample numbers,
crimeware is generally trending upwards

Uppercase

is crimeware prevalence increasing?

> Instances of crimeware have grown steadily, year over year. The prevalence and frequency of crimeware has desensitized security teams and crimeware fatigue is a threat to organizations. As a result, crimeware poses a more likely business impact threat than sophisticated attacks.

crimeware is generally trending **upwards.** different families experienced ups and downs, the overall data indicates there continues to be more crimeware as time progresses. **2017 and 2018 saw enormous increases across the board when compared to the previous three year**s. Generally, each assessed category consistently fell above the median count of samples (**400K) by Q2 of 2017**, with a small dip in infostealers in Q3 of 2017.

[DEPENDING ON TIME]

Bankers
During the first three years of study (2013-2017), banker growth was relatively flat and ranged from between 104,000 distinct samples up to 362,000 samples per quarter. The second quarter of 2017 saw banker malware increase more than **1130%**. While this increase is staggering, it was not sustained and bankers quickly fell back to a

mere **230%** above the old record high set in Q3 of 2013. After the soaring heights of 2017, bankers leveled out by the start of 2018 and slowly decreased approaching the average of 720,000 samples as the year progressed.

Ransomware

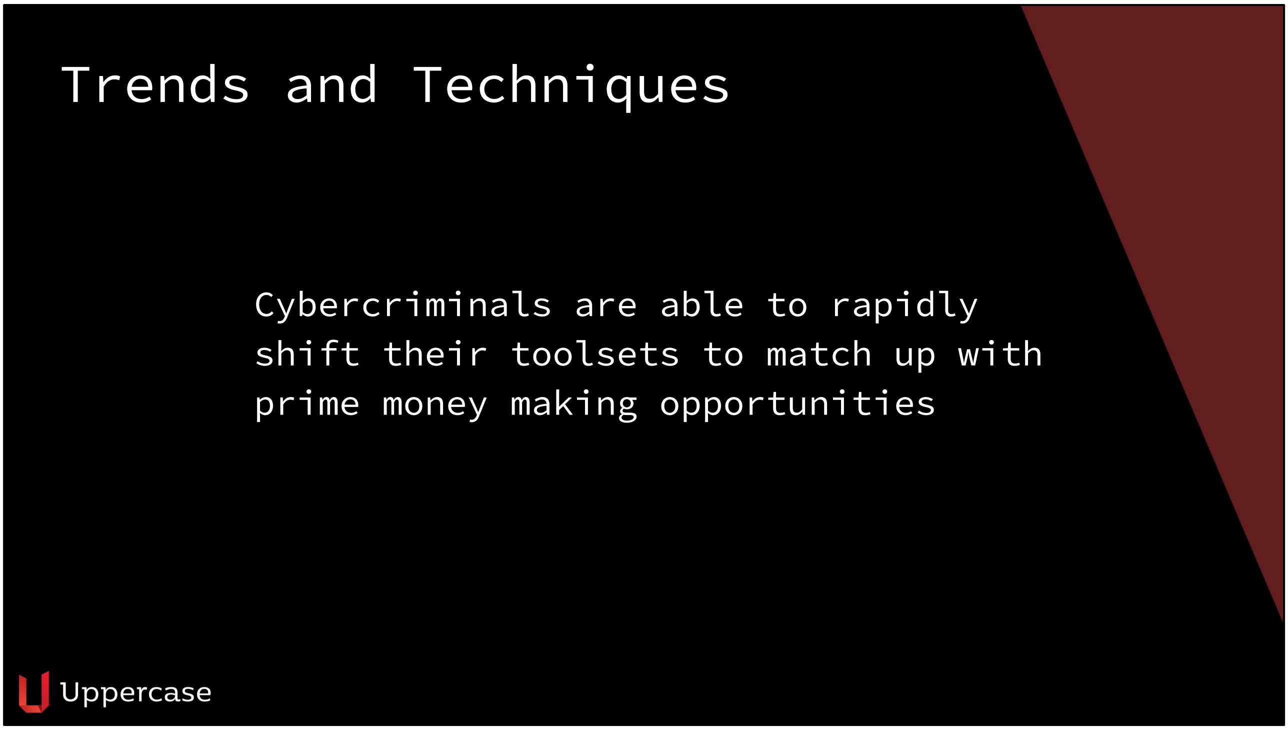
Ransomware followed a more reliable growth track than all other evaluated crimeware types. In 13 of 20 quarters (65%) ransomware counts increased. Ransomware surpassed information stealers by Q2 of 2014 and bankers by Q4 of 2014 and continued a general increase, reaching its apex in Q3 of 2017. From its lowest point of 140,000 distinct samples in Q2 2014 to its highest point of more than 4.1 million samples in Q4 2017, ransomware grew more than **2,800%**. Like bankers, this massive growth was not sustained, but despite a correction by Q1 2018 and a valley in Q2 of 2018, growth once again trended upwards by the end of the year, surpassing the average of 1.29 million distinct samples.

Infostealers

Dedicated information stealers saw consistently stable numbers from 2013 through 2018. From its high point of 1.4 million samples in Q3 2013 to its low point of 159,000 samples in Q1 2016, infostealers saw a decrease of more than **88%**. Like other crimeware categories, its lowest low presaged a period of stable, flat growth until dipping again towards the average of 550,000 samples in Q4 2018.

Miners

Miners were relatively uncommon until the transition from 2017 to 2018. From its lowest point of 18,500 distinct samples in Q1 2013 to its highest point of 5.5 million samples in Q1 2018, miners saw a staggering growth of more than **29,000%** over the entire dataset**.** The bulk of this growth, **6,000%,** occurred between Q3 2017 and Q1 2018, a period of only 6 months. Miners would rapidly fall from their apex, decreasing by more than **74%** in a single quarter from Q1 2018 to Q2 2018. Despite a plummet from its highest peak, the overall surge in growth which took place, combined with a smaller growth spurt between Q2 and Q3 of 2018, kept miners above the average of 520,000 samples.

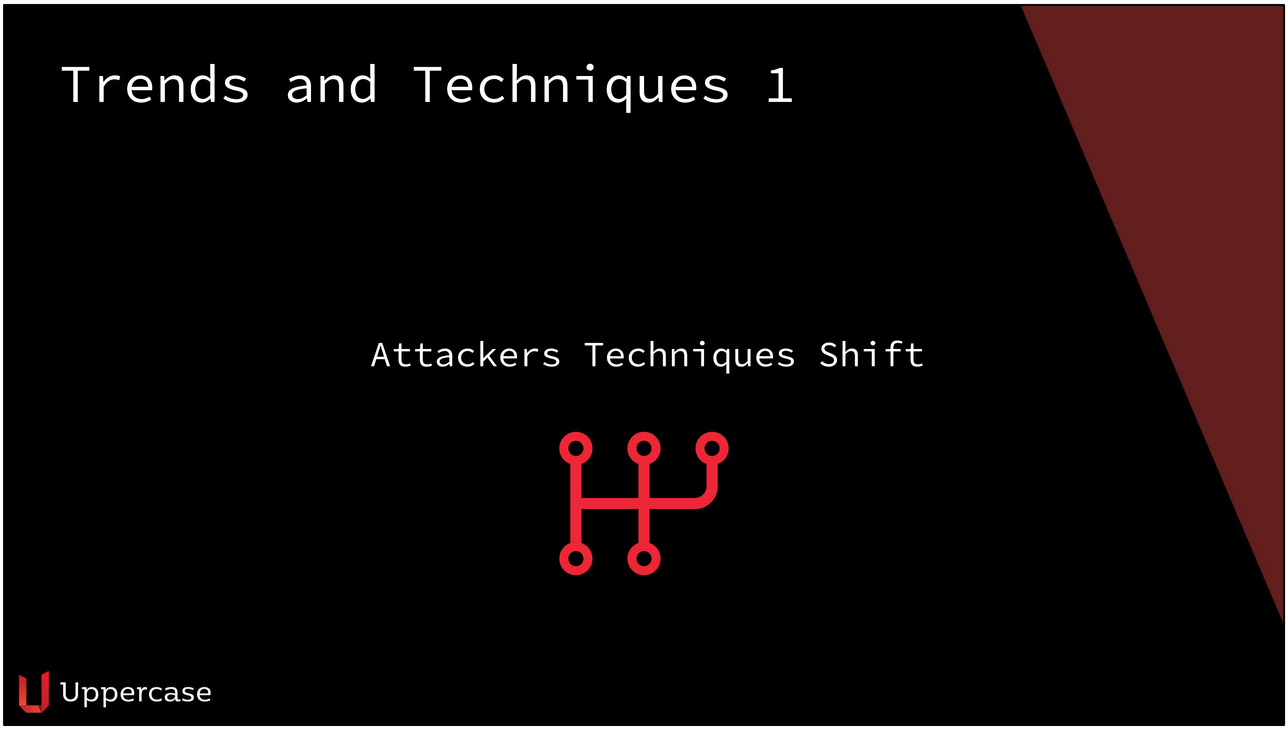


Trends and Techniques

Cybercriminals are able to rapidly shift their toolsets to match up with prime money making opportunities

Uppercase

The interplay between discrete monetization techniques and boom/bust cycles of crimeware families is abundantly clear when examining the overall data overlaid with historical context. Each crimeware category peaked while others' growth slowed, suggesting a relationship between the proliferation of tactics and malware variety of choice by threat actors. Typically within a 3 month period, **cybercriminals are able to rapidly shift their toolsets to match up with prime money making opportunities**.



Trends and Techniques 1

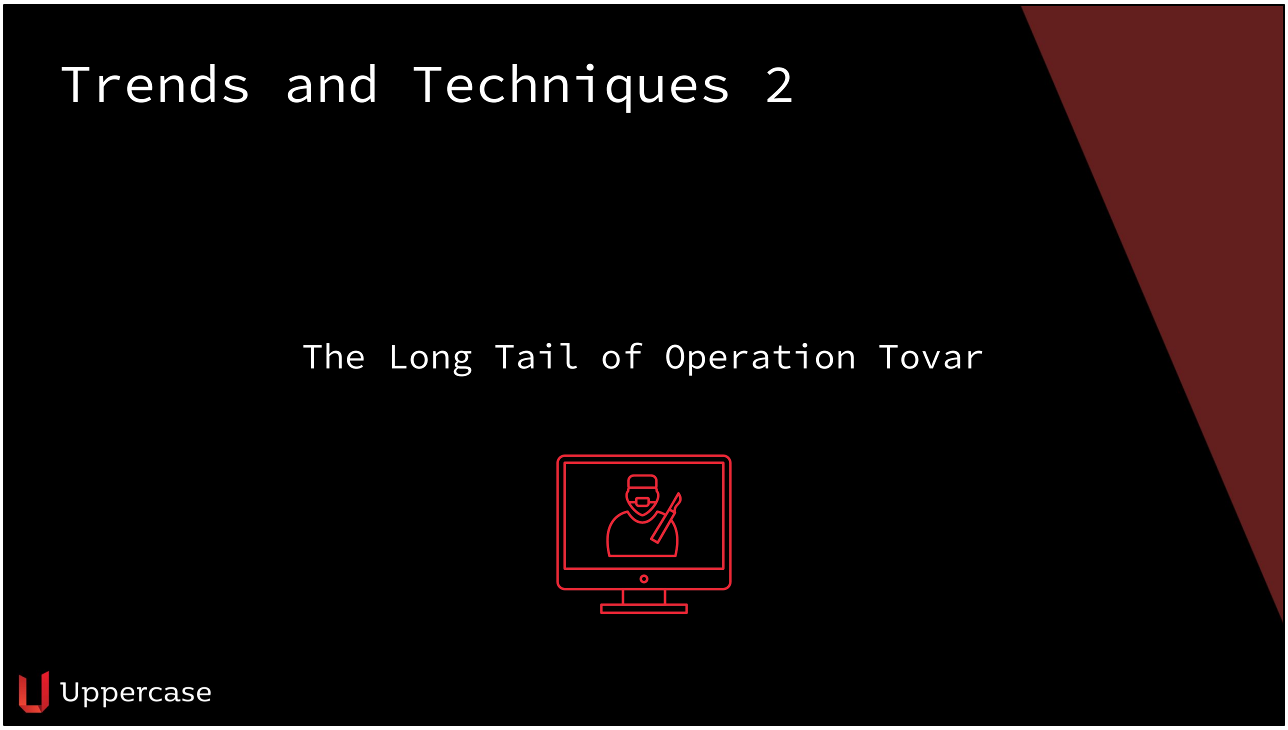
Attackers Techniques Shift

Uppercase

do trends reflect the propagation of techniques?

Crimeware is a business. Threat actors model their workflow and operate using traditional enterprise workplace standards in order to achieve maximum profit. For example, the push towards consolidation and “crimeware-as-a-service” demonstrates an ability to scale profitable enterprises while leveraging new infection methods. Typically within a three-month period, cybercriminals are able to rapidly shift their toolsets to align with prime money making opportunities. For example:

- **Cryptomining as an operation --** The bull market run of cryptocurrencies, as best mapped by the Bitcoin Index, reached its peak at the end of 2017 and began to crash by February of 2018. Following this trend, cryptominer activity dropped by more than 50% over the course of the year. The correlation between spikes in the Bitcoin Index and popularity of miners demonstrates that criminals viewed cryptocurrency as a fertile business opportunity.



Trends and Techniques 2

The Long Tail of Operation Tovar

Uppercase

do trends reflect the propagation of techniques?

Financially motivated threat actors demonstrated a remarkable ability to identify windows of opportunity in which to use specific monetization techniques to great effect, likely in response to threats against their operations. This was particularly potent in the case of ransomware. Ransomware's genesis preceded the initial years of our study by 24 years, but not until the collapse of Cryptolocker in Q2 2014 did the crypto ransomware variants really take off. One of the key events contributing to the increase in ransomware prevalence is the dismantling of the GameOver Zeus botnet in "Operation Tovar." GameOver Zeus was the premier mechanism for distributing the most successful ransomware of its era, Cryptolocker. By leveraging an existing network of machines compromised by GameOver Zeus, Cryptolocker earned $3 million for its operators despite an estimated 1.3% payment rate. The takedown of GameOver Zeus created a power vacuum that was quickly filled by opportunistic attackers who deployed their own versions of ransomware, with the first juggernaut on the scene being CryptoWall, which potentially earned as much as $325 million in bitcoin by 2015, just one year after its emergence and subsequent dominance of the addressable market space. But what changed in 1 year to cause such a massive earnings differential? **Distribution channels**. Ransomware operators after Cryptolocker no longer limited their operations to already compromised devices but instead made use of a wide variety of deployment tactics including exploit kits and malspam. This amplified the reach of ransomware by massively increasing the number of potential victims. Even with sub 1% payment rates, the sheer mass of ransomware compromises quickly piled up.

Trends and Techniques 3

Adjusting to Threats

Uppercase

do trends reflect the propagation of techniques?

A secondary effect of the Operation Tovar takedowns on ransomware was the increased risk involved with operating traditional banking malware. GameOver Zeus' demise signaled to financially motivated threat actors that law enforcement was willing and able to pursue action against them. The increased risk of operating a banking malware enterprise may have spurred the shift to ransomware in the proceeding years. Ransomware requires minimal infrastructure; in fact, the biggest overhead derives from customer service to help victims navigate TOR, cryptocurrency conversion, and payment. The shift to ransomware also shortens the path to profit realization for operators: instead of having to move cash out of victim bank accounts into mule networks for laundering, threat actors could launder cryptocurrency via various exchanges and then "cash out." This increased velocity of tangible gains may have contributed to the growth in both ransomware families and the scale of ransomware operations. This trend continued until 2017, which saw a decrease in ransomware potentially due to an over-saturation of the market.

Trends and Techniques 4

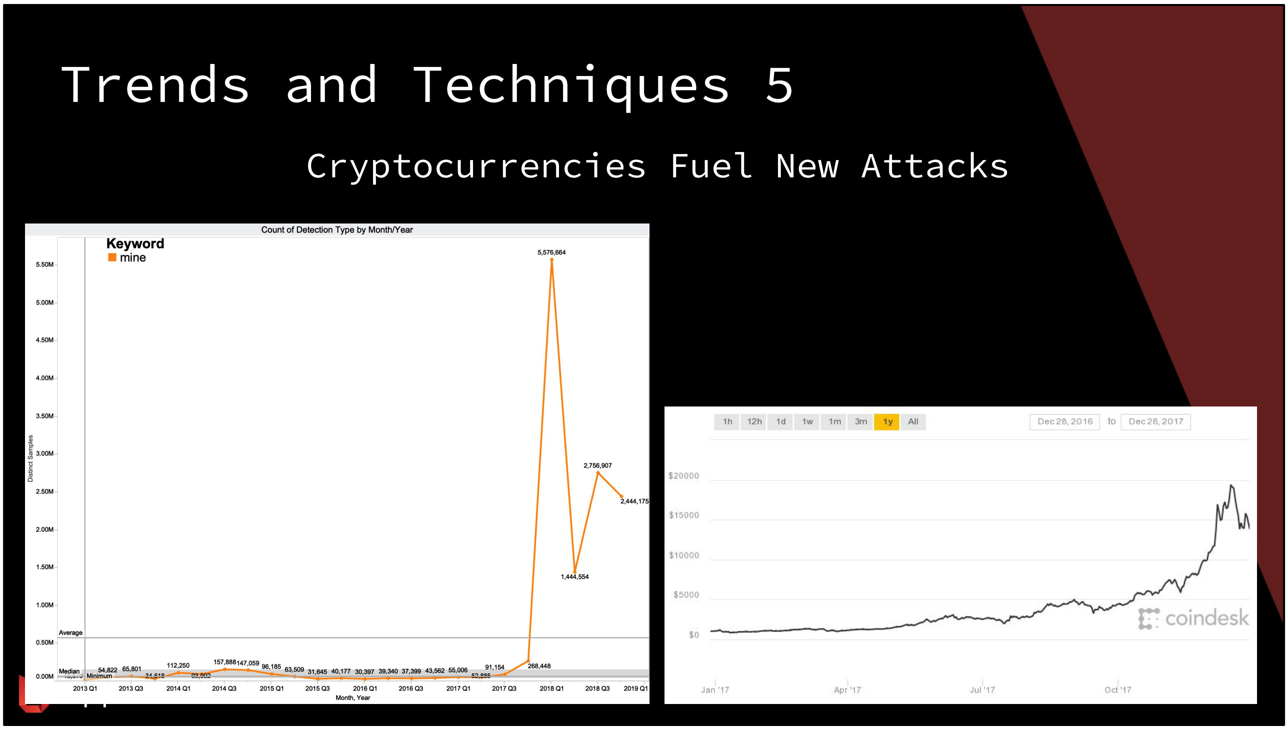
Corporations Under Attack

Uppercase

do trends reflect the propagation of techniques?

- **Sophistication arose from the opportunity granted by volume** -- Deploying crimeware is inexpensive and low-effort for financially-motivated actors. As a result, attackers have optimized for volume and speed. High volumes of broadly-cast attacks over time enabled financially motivated adversaries to optimize attack campaigns towards the most lucrative targets. Increased operationalization and strategy has resulted in increasingly sophisticated and targeted crimeware.
- **Corporations as targets --** As threat groups increased attack sophistication, organized criminal groups that initially targeted consumers switched to deploying new tactics to compromise corporate victims.

By the end of 2017, organized criminal crews would revive one old tactic [with a twist] and pioneer a new one for effective ransomware deployment against **corporate victims**. First, the threat actors operating one of the larger Dridex affiliates began to selectively target already compromised victims for BitPaymer deployment. Once a victim was selected, the operators would manually deploy their ransomware payload for maximum effect.. While this tactic may harken back to the deployment methodology of CryptoLocker, i.e. manual payload deployment post compromise, BitPaymer differs in that the targets are specifically selected for maximum impact. This tactic was later emulated by one of the TrickBot affiliates who used the Ryuk ransomware in much the same way. The new tactic brought to the fore sought to abuse weak external accessibility controls such as Remote Desktop Protocol (RDP) to allow attackers to gain footholds on corporate networks. The operators of SamSam were one of the first to leverage this tactic to establish a bastion within a corporate environment and then pivot laterally to identify ideal, lucrative targets. Combined, these two techniques, termed “Big Game Hunting” by CrowdStrike, spread to numerous organized threat actor groups and continue to be devastatingly effective well into the current era. Ultimately, this tactic shift may have been precipitated by the increase in corporate asset compromises by major crimeware players who subsequently realized they could take advantage of innumerable attack vectors that saw glacial rates of remediation.



Trends and Techniques 5

Cryptocurrencies Fuel New Attacks

do trends reflect the propagation of techniques?

If the growth of ransomware demonstrates how threat actors responded to both law enforcement pressures and a need for a shorter cashout cycle, mining malware demonstrates how threat actors can quickly respond to, and capitalize on changes at, a global economic scale. This can be demonstrated by comparing the growth in bitcoin value (the best indicator of overall cryptocurrency performance) with that of mining malware detections.

As the graphs above indicate, the rise in value of bitcoin is reflected by the rise in mining malware. Several technical factors come into play that influenced this swift growth:

Automated scanning and exploitation botnets, which previously dropped DDoS tools, opted instead for miners.

1. The barrier to entry for having a ready to go miner payload is extremely low. Many open source miners can be freely downloaded. Miners aren’t illegal, its their intent that makes them malware (abuse of resources).
2. Miners are multi-OS, including Android. Typically financial malware predominantly targets Windows or Android. Unix-based OS targeting is particularly interesting, as these operating systems are very commonly found

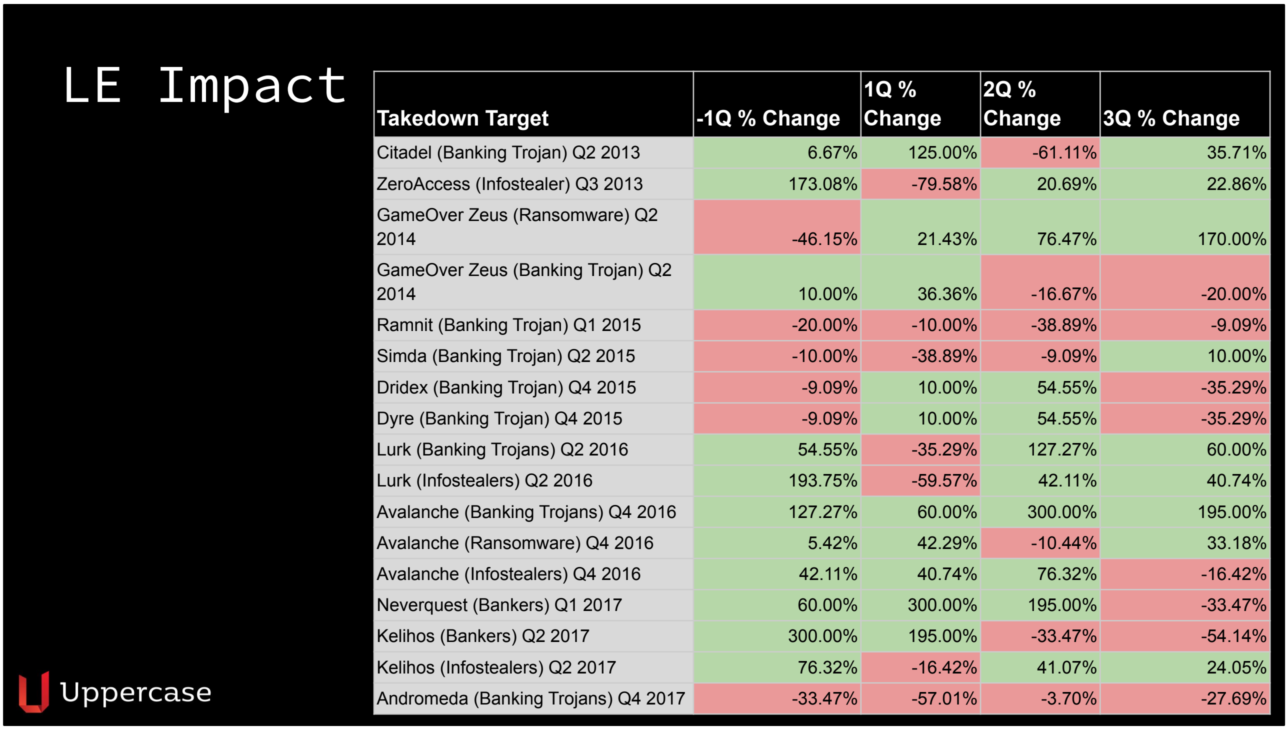
1. in data centers. Miners want compute power; what's better than a server?
2. Browser based miners, such as the prolific coinhive, contributed the most to overall growth of mining malware. Tiny Javascript snippets, which are platform agnostic, are all it takes to turn a vulnerable website into a mining machine that abuses all of its visitors. This can be seen in Drupalgeddon 2, in which the vulnerable CMS was globally exploited to add browser based mining scripts.

These technical factors, combined with the massive increase in cryptocurrency values and a foreshortened realization of profits, spawned a gold rush which many actors, large and small, embraced.

Finally we come to the banking trojans and infostealers: the tried and true tools that will likely never disappear. It is likely the waning popularity of bespoke infostealers and the later growth of banking trojans, which began in Q1 2017, is driven by the convergence of both capabilities into singular malware packages. Dedicated infostealers' path to profit realization involved the following basic tenets:

1. Actors must gather and exfiltrate all the data from a compromised host.
2. Operators must then sift through the data to identify credentials or other resources of value.
3. The data must then be prioritized for sale via different avenues (forums, chat groups).
4. External customers must actually buy the data in a timely fashion for it to be relevant.

The path to profit for infostealers is long; even with the advent of automatic account checkers to insure data is “fresh”, multiple steps must be taken for an operator or group to see any cash returns. This likely has contributed to the shift towards more modular malware frameworks such as Dridex, Emotet, GozNym, and Trickbot, that incorporate infostealer and banking trojan components. Modular frameworks have the added benefit of allowing operators to select only the tools and capabilities they need to get the data they believe is of highest value.



LE Impact

Takedown Target	-1Q % Change	1Q % Change	2Q % Change	3Q % Change
Citadel (Banking Trojan) Q2 2013	6.67%	125.00%	-61.11%	35.71%
ZeroAccess (Infostealer) Q3 2013	173.08%	-79.58%	20.69%	22.86%
GameOver Zeus (Ransomware) Q2 2014	-46.15%	21.43%	76.47%	170.00%
GameOver Zeus (Banking Trojan) Q2 2014	10.00%	36.36%	-16.67%	-20.00%
Ramnit (Banking Trojan) Q1 2015	-20.00%	-10.00%	-38.89%	-9.09%
Simda (Banking Trojan) Q2 2015	-10.00%	-38.89%	-9.09%	10.00%
Dridex (Banking Trojan) Q4 2015	-9.09%	10.00%	54.55%	-35.29%
Dyre (Banking Trojan) Q4 2015	-9.09%	10.00%	54.55%	-35.29%
Lurk (Banking Trojans) Q2 2016	54.55%	-35.29%	127.27%	60.00%
Lurk (Infostealers) Q2 2016	193.75%	-59.57%	42.11%	40.74%
Avalanche (Banking Trojans) Q4 2016	127.27%	60.00%	300.00%	195.00%
Avalanche (Ransomware) Q4 2016	5.42%	42.29%	-10.44%	33.18%
Avalanche (Infostealers) Q4 2016	42.11%	40.74%	76.32%	-16.42%
Neverquest (Bankers) Q1 2017	60.00%	300.00%	195.00%	-33.47%
Kelihos (Bankers) Q2 2017	300.00%	195.00%	-33.47%	-54.14%
Kelihos (Infostealers) Q2 2017	76.32%	-16.42%	41.07%	24.05%
Andromeda (Banking Trojans) Q4 2017	-33.47%	-57.01%	-3.70%	-27.69%

Uppercase

How do global LE actions affect crimeware proliferation?

- **The efficacy of law enforcement efforts decreases over time -** Financially motivated actors' ability to adapt to countermeasures outpaces the ability of traditional law enforcement to find and prosecute criminals. Financially motivated actors model risk based on law enforcement efforts, and adapt attack techniques based on profit. As a result of time, geographical and other factors that limit law enforcement efforts, crimeware operations have more time to adapt and make crimeware progressively more detrimental.

Typically, within 2 quarters, malware sample counts which were impacted by a given takedown show definitive indications of growth

In **41%** of the takedown attempts we covered in this study, the affected malware type decreased within one quarter. When takedowns appeared to have an impact on raw sample counts, **43%** of instances were preceded by a downward trend in the previous quarter. Within one quarter following a decrease in samples, **57%** of crimeware types showed signs of growth. Within two quarters, this number rose to **71%**.

Table 1. Some takedowns affect multiple types of crimeware and are thus separated out for a net total of 15 takedowns. Each row label is the target of a takedown, the applicable malware

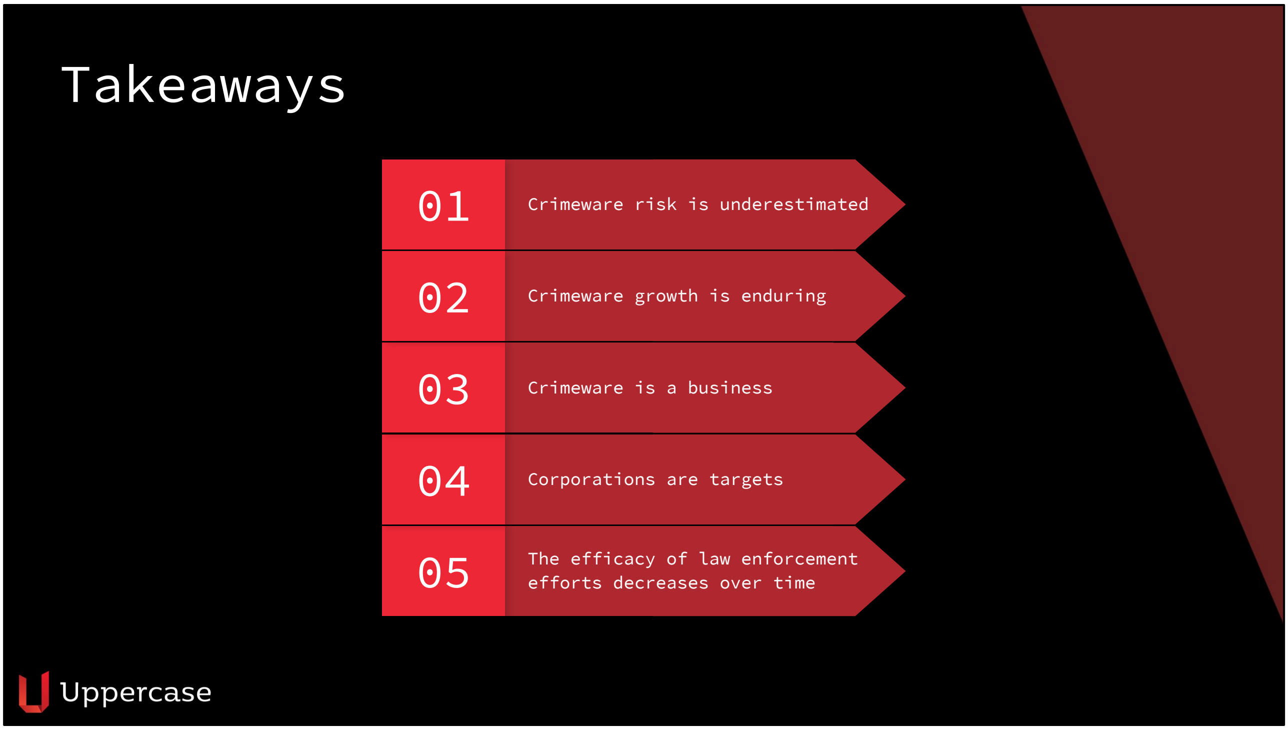
category, and the quarter in which the takedown occurred. This table shows the quarter over quarter percentage change in sample count as compared to the quarter prior to a takedown and over the next 3 quarters following a takedown. Most takedowns targeted banking trojans, though some had ancillary effects on other types of crimeware.

-1Q => Change from Quarter Prior compared to Quarter in Which Takedown Occured

1Q, 2Q, 3Q => %change from prior quarter to next quarter

Takedowns may also have had an added side effect of pushing financially motivated threat actors to utilize completely new tools and techniques to continue operation: this can be seen in the generalized growth of ransomware following the takedown of GameOver Zeus in 2014

Law enforcement operations are frequently hobbled by outdated laws and complex barriers to cooperation with the private sector, though the increasing frequency of arrests instead of disruptions is a positive sign of both the willingness and the capability to act against cyber criminals. It is likely, however, that recent actions against cyber criminals have had the effect of “culling the herd” rather than impacting organized operations. Future efforts should continue to involve the private sector but need to be focused on agility. Efforts should also be targeted against operators rather than infrastructure as illustrated by the general ineffectiveness of both the Lurk and Avalanche takedowns. Finally, increased frequency of action against cyber criminals could reduce their ability to adjust to legal intervention. Otherwise, defenders will continue to be on the back foot.



Takeaways

01 Crimeware risk is underestimated

02 Crimeware growth is enduring

03 Crimeware is a business

04 Corporations are targets

05 The efficacy of law enforcement efforts decreases over time

Uppercase

Crimeware is a cornerstone to financially motivated threat actors' toolsets and sees consistent and continuous evolution in its operation. Crimeware developers have demonstrated resilience in the face of an evolving security landscape and law enforcement actions through constant shifts and updates to their tools, techniques, and procedures. This has resulted in a perennial back and forth between criminally-minded attackers and budget-constrained defenders.

- **Crimeware risk is underestimated --** Misconceptions around the severity of risk from financially motivated threat actors has hobbled enterprise defense efforts. Rates of losses due to crimeware are climbing, and countermeasures are decreasing in efficacy. Crimeware as a financial risk quantifiably outranks more sophisticated threats such as APTs. The ability of crimeware to disrupt businesses is tremendous and if efforts are not increased, there will be attacks greater in impact, scale and cost.

- **Crimeware growth is enduring** - Instances of crimeware have grown steadily, year over year. The prevalence and frequency of crimeware has desensitized security teams and crimeware fatigue is a threat to organizations. As a result, crimeware poses a more likely business impact threat than sophisticated attacks.

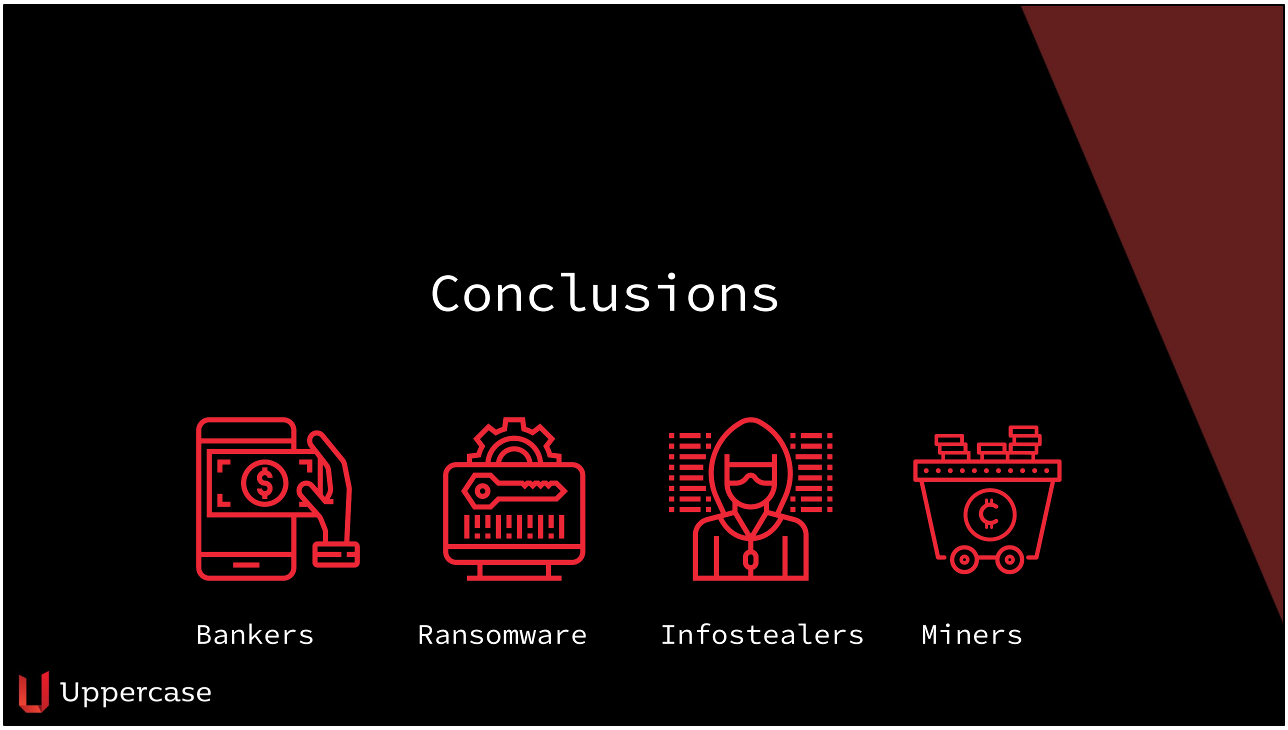
- **Sophistication arose from the opportunity granted by volume** -- Deploying crimeware is inexpensive and low-effort for financially-motivated actors. As a result, attackers have optimized for volume and speed. High volumes of broadly-cast attacks over time enabled financially motivated adversaries to optimize attack campaigns towards the most lucrative targets. Increased operationalization and strategy has resulted in increasingly sophisticated and targeted crimeware.

- **The efficacy of law enforcement efforts decreases over time -** Financially motivated actors' ability to adapt to countermeasures outpaces the ability of traditional law enforcement to find and prosecute criminals. Financially motivated actors model risk based on law enforcement efforts, and adapt attack techniques based on profit. As a result of time, geographical and other factors that limit law enforcement efforts, crimeware operations have more time to adapt and make crimeware progressively more detrimental.

- **Crimeware is a business**. Threat actors model their workflow and operate using traditional enterprise workplace standards in order to achieve maximum profit. For example, the push towards consolidation and "crimeware-as-a-service" demonstrates an ability to scale profitable enterprises while leveraging new infection methods. Typically within a three-month period, cybercriminals are able to rapidly shift their toolsets to align with prime money making opportunities. For example:

    - **Cryptomining as an operation --** The bull market run of cryptocurrencies, as best mapped by the Bitcoin Index, reached its peak at the end of 2017 and began to crash by February of 2018. Following this trend, cryptominer activity dropped by more than 50% over the course of the year. The correlation between spikes in the Bitcoin Index and popularity of miners demonstrates that criminals viewed cryptocurrency as a fertile business opportunity.

- **Corporations as targets** -- As threat groups increased attack sophistication, organized criminal groups that initially targeted consumers switched to deploying new tactics to compromise corporate victims.



Conclusions

Many cyber security practitioners discount the threat of financially motivated threat actors due to the misunderstanding that countermeasures successfully prevent these commodity threats. Unfortunately, frequency does not seem to increase defensive efficacy: crimeware is a larger threat now than it was 6 years ago, especially to businesses. The losses continue to mount: for the US in 2018, the FBI estimates a total loss of 2.4 billion dollars, a massive increase from the estimated 1.25 billion dollars in losses from 2017.

Crimeware is **noisy**. Individuals and corporations alike are bombarded by malspam and drive-bys and the prevalence is growing. Organizations falsely believe that because crimeware is so common, defensive solutions can adequately combat it. The frequency of crimeware iteration in everything from delivery and distribution techniques, to countermeasures, to modules, far outpaces reactive industry practices. Cyber criminals typically rely on a volumetric approach to gain a foothold; whether malspam or driveby, it is inexpensive and low effort to run a malware campaign. Financially motivated threat actors have realized they can **frequently land payloads in corporate environments**. This has led to the expansion of targeted ransomware deployments; often to devastating effect. The continued success of financially motivated threat actors indicates that threats are not required to be advanced to be overwhelmingly successful. The overall growth rate of crimeware indicates that persistence of effort pays off.

Cyber criminals have shown a ready willingness and capability to **rapidly evolve monetization techniques**. Whether from mimicry or organic competition, infostealers, bankers, ransomware, and miners exploded with variants throughout the course of our study. This evolution is typically spearheaded by key innovations or opportunities in the addressable market space or as a reaction to threats against particular operations. Threat actors have shifted multiple times in the past six years to follow trends: this is most readily apparent in the enormous uptick in dedicated mining malware and the changes in ransomware deployment tactics. This has culminated in the current converged environment in which malware tools have multiple, overlapping capabilities and can be leveraged based on attacker orientation: the most notable of which is targeted ransomware deployments employed by multiple cyber criminal organizations that are commonly facilitated by modular banking trojans as a beachhead. The tools and techniques we are seeing now have clear roots in previous generations of financially motivated malware campaigns.

Commonly passed over and erroneously labeled as commodity, crimeware can no longer be ignored as a mere “one trick pony.” Crimeware is no longer a single pronged threat. What was “just a banker” in the past now has modular adaptive capabilities that can allow threat actors to capitalize on its environment. This orientation is critical for attackers to best leverage their access. Cyber criminals operate as business enterprises: they adapt to threats against their operations, they follow the market, they invest in R&D, they operate with a malleable playbook, and they leverage “as-a-service” models to streamline operations. In the case of some organizations, campaigns are solely conducted on M-F during Western working hours, to maximize impact.

Diminishing returns of law enforcement actions combined with the mounting losses attributed to financially motivated threat actors indicate that historical approaches to enforcing laws are losing effectiveness. The “single point of failure” has fallen out of fashion in the age of crimeware as a service. Cyber criminals are better able to protect themselves and their businesses from technical disruption by distributing infrastructure, dividing specializations, and establishing redundant and resilient operations. Private industry and global law enforcement must act with greater agility when mounting technical disruptions and kinetic action against cyber criminals. The lag time between discrete actions provides a massive gap in which threat actors are able to recover. Reducing this window of opportunity may increase the efficacy of takedowns and arrests.

Over the course of our study, Chronicle researchers have identified numerous trends and evolutions in crimeware. Over the course of our research we clearly saw monetization techniques proliferate as the criminal market identified new opportunities or was pressured by external entities. However, the efforts that have historically been undertaken to combat crimeware are becoming increasingly less effective. Unfortunately, many security practitioners consider financially motivated malware as a lesser threat when compared to their nation state counterparts and thus opt to focus on the later. This is, unequivocally, to the detriment of overall defensive posture. Crimeware is the most prolific malware based threat facing not only individuals and home users, but also massive multi-national corporations, and it is becoming increasingly more damaging. The convergence of previously discrete functionality into modular malware frameworks combined with the ability to reliably establish bastions within corporate networks has allowed modern malware operations to have devastating effects on corporations throughout the world. Financially motivated threat actors understand the value of their targets: they can accurately orient themselves to make use of their access. Despite a general lack of attention, crimeware isn’t going away; it will continue to grow more capable as operators further refine and streamline their operations.

Thank You

Contact:
blevene@chronicle.security

Uppercase

The paper will be available as this presentation finishes (or maybe before). All data will be available on github when the paper is published.

https://github.com/Blevene/Crimeware-In-The-Modern-Era