RSA

TRENDING THE CRIMEWARE ECOSYSTEM

Kevin Stear
Threat Analysis Lead
RSA FirstWatch
@w1mp1

THE CRIMEWARE ECOSYSTEM

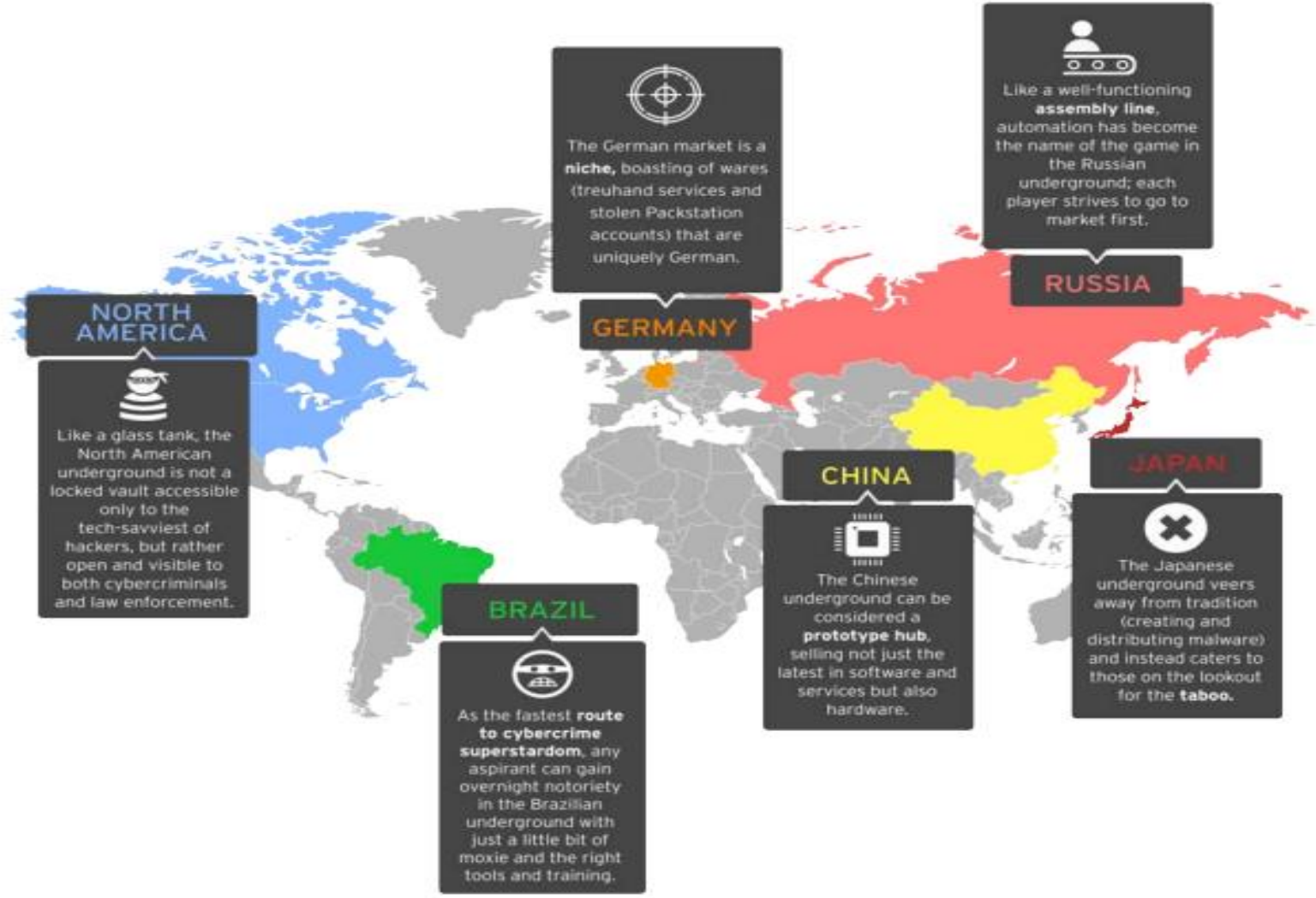
ABSTRACT

Capitalism and **open market forces** currently drive the evolution of today's **Crimeware environment**, where a close-knit ecosystem of goods and services is thriving based on demand from ongoing malicious campaigns.

THE CRIMEWARE ECOSYSTEM

UNDERGROUND FORUMS AND EXCHANGES

- Underground forums currently occupy several regional network and market segments
- Emerging W. Africa marketplace
  - Real Nigerians?
- Forums act as key exchanges for Crimeware goods and services
  - Traffic/Delivery
  - Hacking-as-a-Service (HaaS)
  - Malware Development
  - Infrastructure-as-a-Service (IaaS)



Graphic courtesy of Trend Micro:
https://documents.trendmicro.com/assets/wp/wp-cybercrime-and-the-deep-web.pdf
https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf

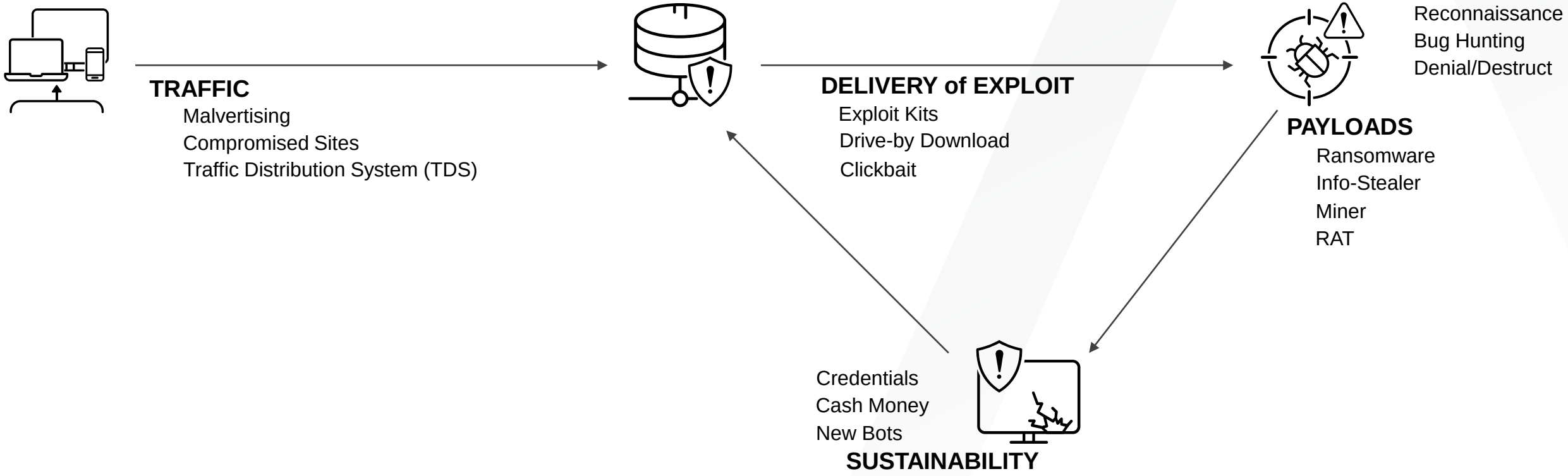
THE CRIMEWARE ECOSYSTEM

GOODS & SERVICES

- **Traffic**
  - Compromised Site
  - Malvertising
  - Spam Provider
  - Traffic Distribution System (TDS)
- **Delivery**
  - Exploit Kit
  - Drive by Download
  - Droppers/Clickbait
- **Hacking**
  - Denial of Service
  - Credential Harvesting
  - Reconnaissance
  - Bug Hunting
- **Malware/Payloads**
  - Ransomware
  - Info-stealer
  - Miner
  - Remote Access Trojan (RAT)
  - Exploit Development
- **Infrastructure**
  - Bulletproof Hosting
  - Shadow Domains
  - Botnets

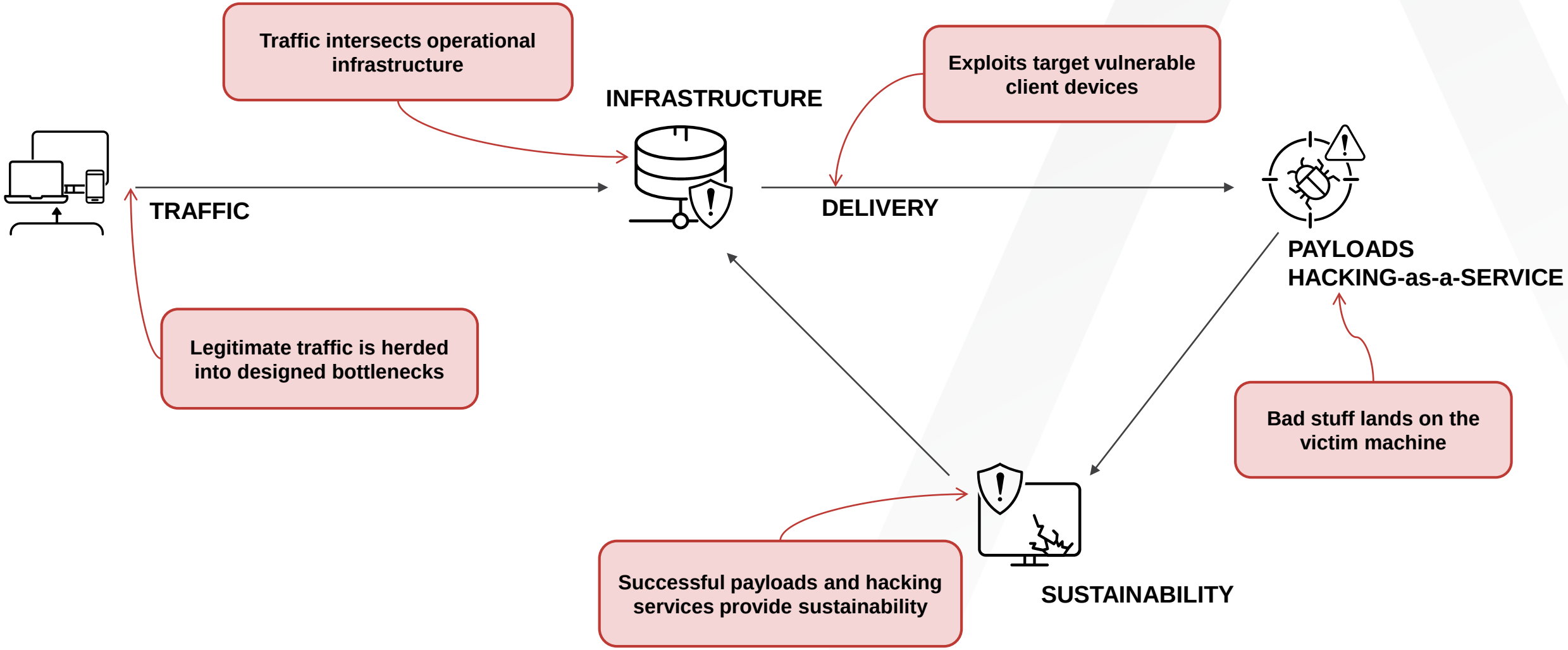
THE CRIMEWARE ECOSYSTEM

HOW IT WORKS TOGETHER



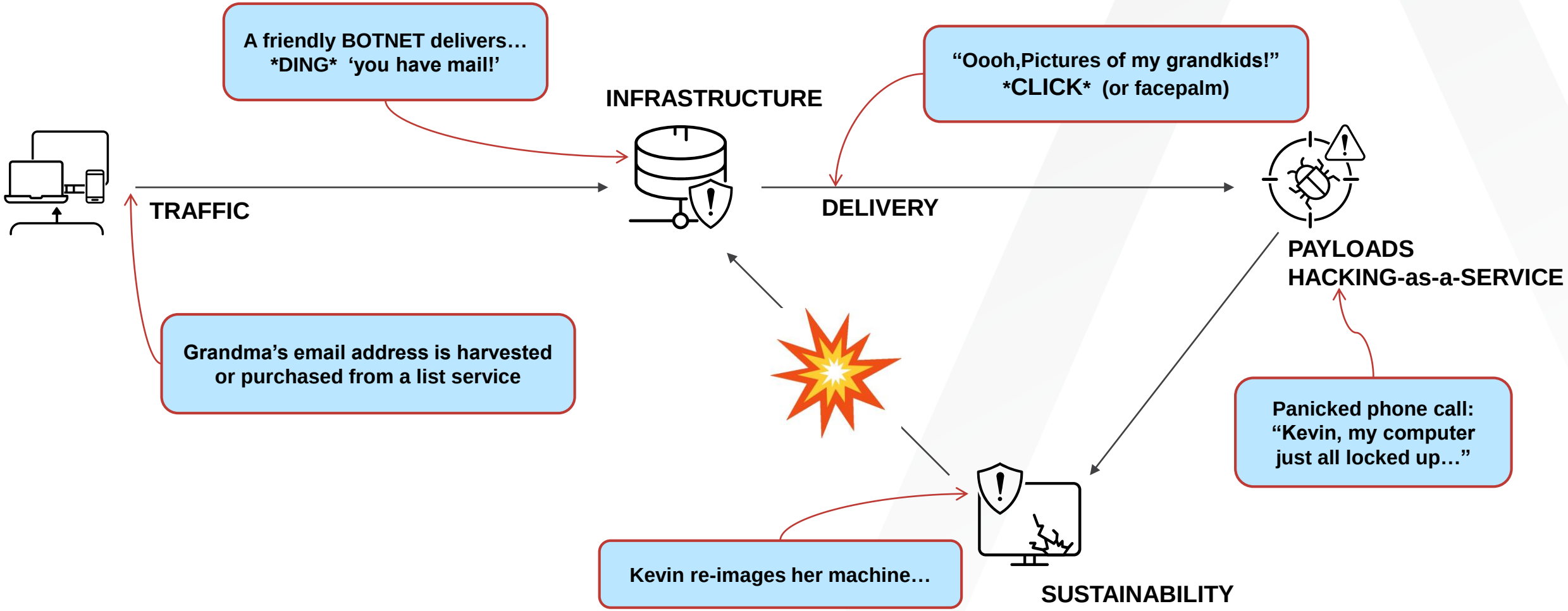
THE CRIMEWARE ECOSYSTEM

HOW IT WORKS TOGETHER – CRIMINAL VIEW



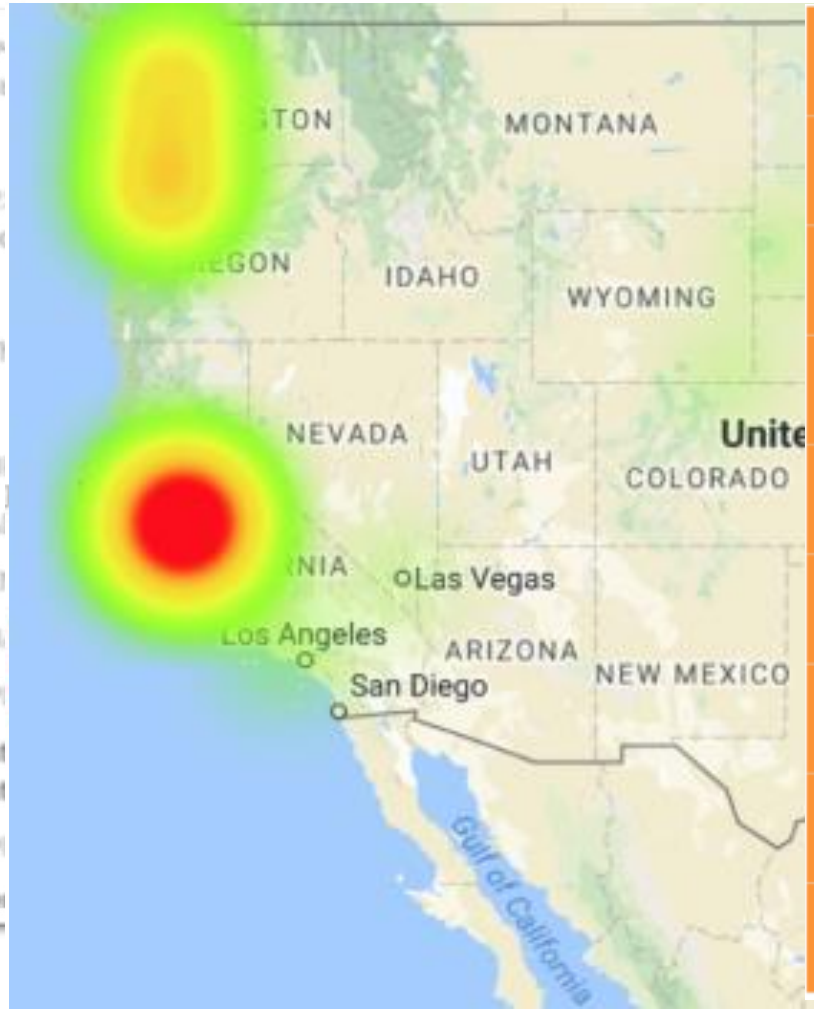
THE CRIMEWARE ECOSYSTEM

HOW IT WORKS TOGETHER – VICTIM VIEW (AKA MY GRANDMA)



CRIMEWARE TRENDS

REALLY… BUT WHY ARE TRENDS IMPORTANT?



	United States	European Union	Asia	Africa
Windows XP	$3 USD	$5 USD	$5 USD	$5 USD
Windows Vista	$5 USD	$7 USD	$6 USD	$6 USD
Windows 7	$8 USD	$8 USD	$7 USD	$7 USD
Windows 8	$9 USD	$10 USD	$9 USD	$9 USD
Windows 10	$9 USD	$10 USD	$9 USD	$8 USD
Windows 2003 Server	$3 USD	$5 USD	$3 USD	$3 USD
Windows 2008 Server	$7 USD	$7 USD	$6 USD	$6 USD
Windows 2012 Server	$8 USD	$9 USD	$6 USD	$7 USD

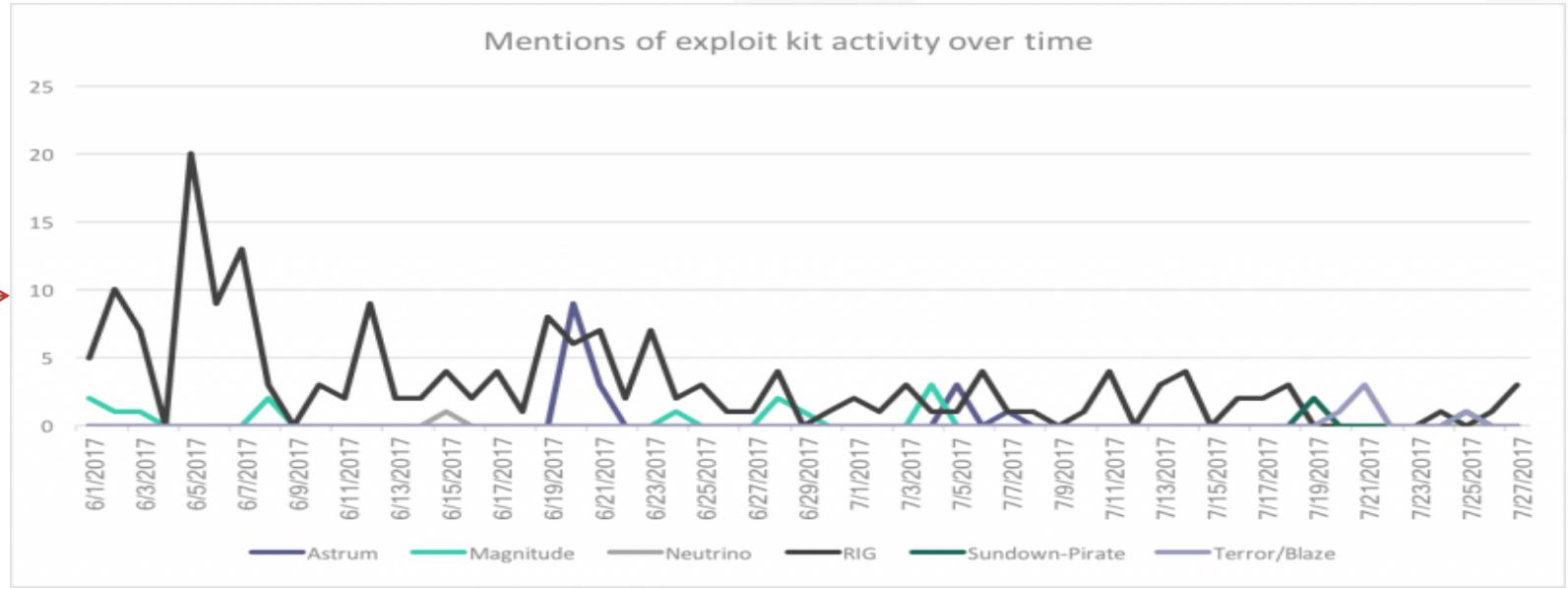
"Ultimate Anonymity Services" Shop Offers Cybercriminals International RDPs: https://www.flashpoint-intel.com/blog/uas-shop-international-rdp-servers/

CRIMEWARE TRENDS

THE DECLINE OF EXPLOIT KITS

- Shadowfall, a joint RSA and GoDaddy takedown
  - Disrupts more than 40,000 active shadow domains supporting RIG Exploit Kit (EK) and other malicious campaigns
- Decline in Exploit Kits?
  - Perceived shift away from compromised sites as a traffic source for EK delivery due to increased scarcity of necessary credentials
  - Industry research support*
- Impact
  - Malspam takes over primary delivery
  - Malvertising becomes primary traffer

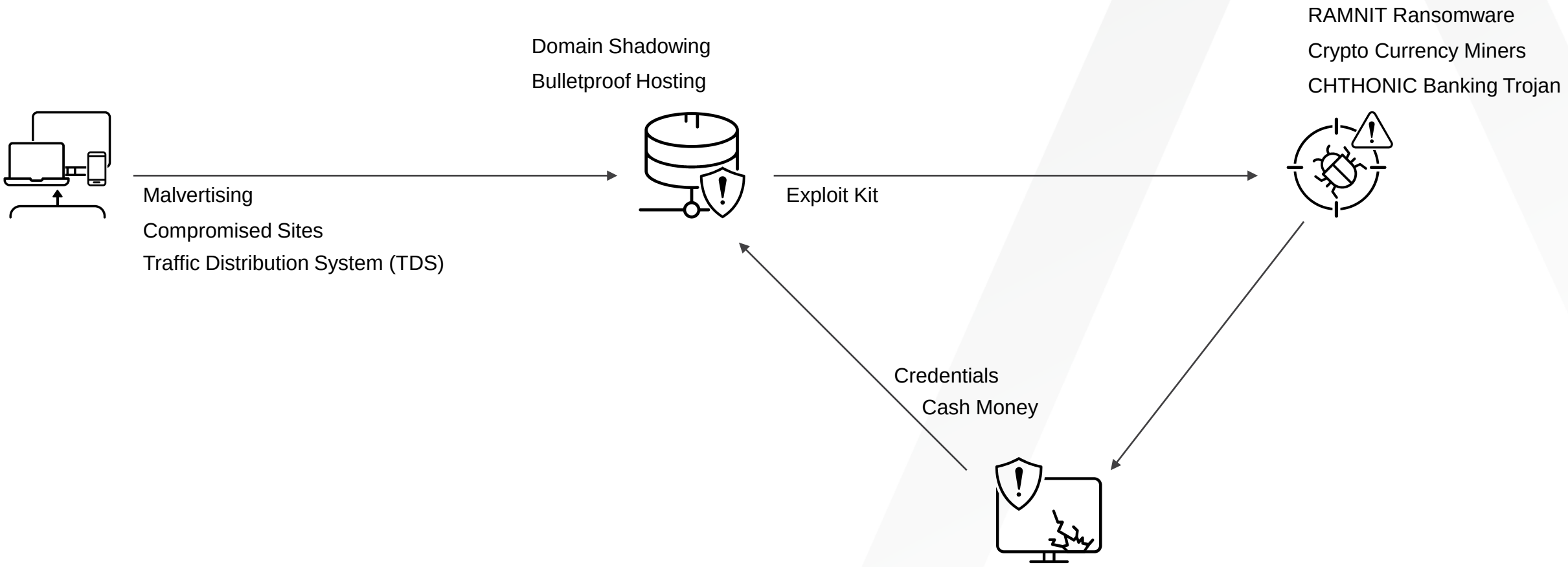
MARKET FORCES AT WORK?



Decline in RIG Exploit Kit: https://researchcenter.paloaltonetworks.com/2017/06/unit42-decline-rig-exploit-kit/
Fluctuation in the Exploit Kit Market – Temporary Blip or Long-term Trend?: https://www.digitalshadows.com/blog-and-research/fluctuation-in-the-exploit-kit-market-temporary-blip-or-long-term-trend/

THE CRIMEWARE ECOSYSTEM

RIG EXPLOIT KIT



CRIMEWARE TRENDS

2017 SUMMER OF MALSPAM

From Jun-Sep 2017, RSA FirstWatch saw the increased use of Malspam as a delivery vector:

- Crimeware:
  - JACKSBOT
  - CVE-2017-8759
  - XMRIG (Miner)
  - ZBOT
  - CVE-2017-0199
  - NANOBOT
  - HANCITOR/PONY
  - LOCKY
  - TRICKBOT
  - GLOBEIMPOSTER
  - BEBLOH
  - CERBER
  - TRICKBOT
  - AGENTTESLA
  - HAWKEYE
  - EMOTET
  - LOCKY
  - LOKIBOT
  - ZYKLON
  - CERBER
  - DRIDEX
- Targeted:
  - MOONWIND
  - COBALT STRIKE
  - CVE-2017-0262
  - DIMNIE
  - CHTHONIC/DIMNIE
  - XTREME
  - MONSOON

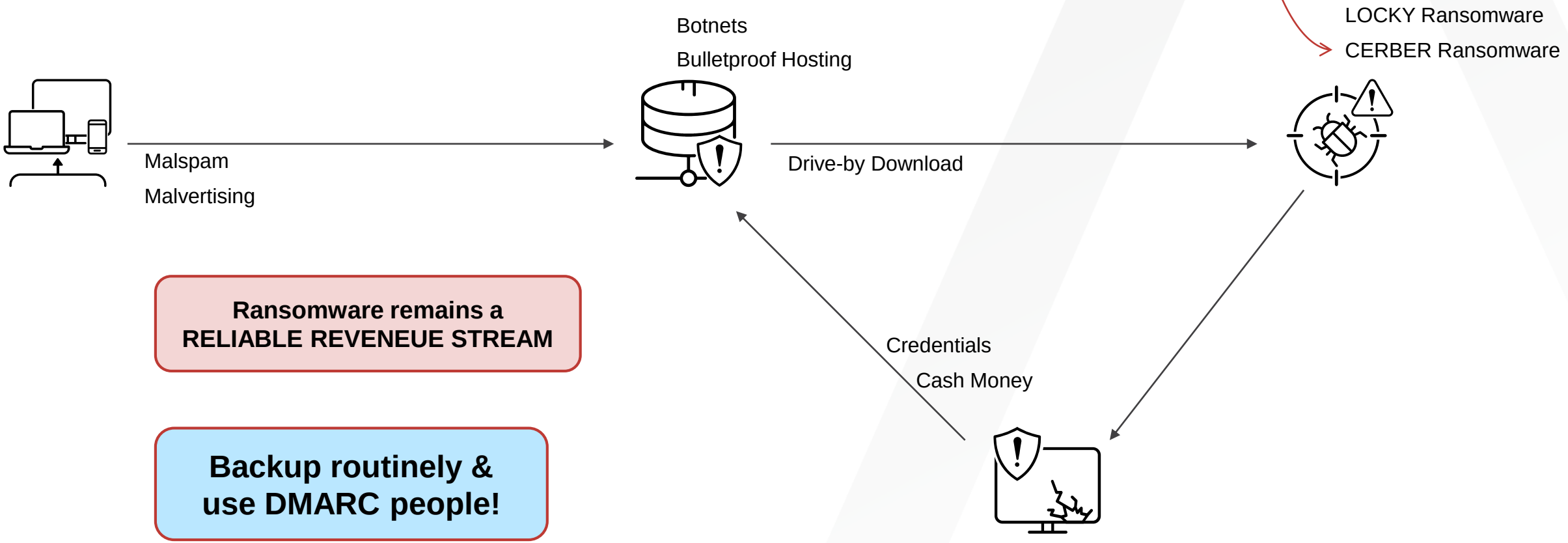
Date	Summary	Details	Email Payload Type	Users Targeted
9/1/2017	Malicious email campaign, morning	"New voice message <digits> in mailbox <digits> from "<digits>" <<digits>>" 7z -> vbs -> locky ransomware	Attachment	2513
9/1/2017	Malicious email campaign, afternoon	"Paypal Security", doc -> trickbot banking trojan	Attachment	31
9/4/2017	Malicious email campaign, morning	"<digits> - True Telecom Invoice for August 2017", link, 7z -> vbs -> locky ransomware	Attachment	614
9/4/2017	Malicious email campaign, morning	"Invoice INV-000868 from Property Lagoon Limited for Gleneagles", 7z -> vbs -> locky and globeimposter ransomware	Attachment	349
9/5/2017	Malicious email campaign, morning	"Scanning", 7z -> vbs -> locky ransomware	Attachment	209
9/5/2017	Malicious email campaign, morning	"New voice message digits in mailbox digits from "digits" <digits>", 7z -> vbs -> locky ransomware	Attachment	25
9/5/2017	Malicious email campaign, morning	"Invoice INV-000338 from Verizon", 7z -> vbs -> locky ransomware	Attachment	22
9/5/2017	Malicious email campaign, morning	"USPS - Holdmail|Confirmation|Document <digits>", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	878
9/5/2017	Malicious email campaign, morning	"eFax", doc -> trickbot banking trojan, continued into 09/08/2017	Attachment	60
9/5/2017	Malicious email campaign, afternoon	"Voice Message from <digits> - name unavailable", link -> js -> locky ransomware, continued into 09/07/2017	Link	8806
9/5/2017	Malicious email campaign, morning	"Eviction warning #<digits>, link -> js -> zeuspanda	Link	5
9/6/2017	Malicious email campaign, morning	"Your invoice for eBay purchases (<digits>#)", link -> js -> locky ransomware	Link	621
9/6/2017	Malicious email campaign, morning	"Your Bill <digits> for domain Document is Ready for Signature", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	901
9/6/2017	Malicious email campaign, afternoon	"Canadian Imperial Bank of Commerce", doc -> trickbot trojan	Attachment	11
9/7/2017	Malicious email campaign, morning	"FreeFax From:<digits>", link -> js -> locky ransomware	Link	198
9/7/2017	Malicious email campaign, afternoon	"Microsoft Store E-invoice for your order #<digits>", link and 7z -> vbs -> locky ransomware	Attachment, link	1554
9/8/2017	Malicious email campaign, morning	"Emailed Invoice - <digits>", html -> js -> locky ransomware and trickbot	Attachment	252
9/11/2017	Malicious email campaign, morning	"Please verify your email address user@domain", link -> js -> trickbot and locky ransomware	Link	2666
9/11/2017	Malicious email campaign, morning	"Missed delivery notification for tracking <characters>", link -> doc -> hancitor -> pony -> evilony -> zloader trojans	Link	834
9/11/2017	Malicious email campaign, morning	"FreeFax From:<digits>", link -> js -> trickbot and locky ransomware	Link	2186
9/12/2017	Malicious email campaign, morning	"FW: Invoice <digits> for accounting services", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	793
9/13/2017	Malicious email campaign, morning	"Incoming RingCentral fax from <digits>", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	834
9/14/2017	Malicious email campaign, morning	"Copy of Invoice <digits>|Voice Message from <digits> - name unavailable", link -> js -> locky ransomware	Link	271
9/14/2017	Malicious email campaign, morning	"Voice Message from <digits> - name unavailable", link -> js -> locky ransomware	Link	2890
9/14/2017	Malicious email campaign, morning	"[Factura: FACV<digits>]", xls -> ursnif/ifsb trojan	Attachment	51
9/18/2017	Malicious email campaign, morning	All subjects contain "invoice", link -> emotet trojan	Link	30
9/18/2017	Malicious email campaign, morning	"Message from KM_C224e", 7z -> vbs -> locky ransomware, continued into 09/19/2017	Attachment	2928
9/19/2017	Malicious email campaign, morning	"HERBALIFE Order Number: <digits>", 7z -> vbs -> locky ransomware	Attachment	1312
9/19/2017	Malicious email campaign, morning	"RE: RE: subpoena", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	1110
9/19/2017	Malicious email campaign, morning	"Emailing - <digits>", 7z -> vbs -> locky ransomware, continued into 09/20/2017	Attachment	2444
9/20/2017	Malicious email campaign, morning	"Your payment #<digits>", 7z -> vbs -> locky ransomware	Attachment	1068
9/20/2017	Malicious email campaign, morning	"Status of Invoice <digits>", rar -> vbs -> locky ransomware	Attachment	275
9/20/2017	Malicious email campaign, morning	"RE: RE: shipping inquiry regarding order", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	781
9/20/2017	Malicious email campaign, morning	"New voice message <digits> in mailbox <digits> from "<digits" <<digits>>", link and 7z -> vbs locky ransomware	Attachment, link	2666
9/21/2017	Malicious email campaign, morning	"Invoice RE-2017-09-21-<digits>, 7z -> vbs -> locky ransomware	Attachment	1119
9/21/2017	Malicious email campaign, morning	"FW: Your Invoice K<digits> from Advanced Maintenance", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	639
9/21/2017	Malicious email campaign, afternoon	Subect contains PIC|IMG|JPG|SCAN, 7z -> vbs -> locky ransomware, continued into 09/22/2017	Attachment	2438
9/22/2017	Malicious email campaign, morning	"Your Invoice # <digits>", 7z -> vbs -> locky ransomware	Attachment	1464
9/25/2017	Malicious email campaign, morning	"Message from <digits>", 7z -> vbs -> locky ransomware	Attachment	4206
9/25/2017	Malicious email campaign, morning	"<digits>_Invoice_<digits>", 7z -> vbs -> locky ransomware	Attachment	4756
9/25/2017	Malicious email campaign, afternoon	"eFax", doc -> trickbot banking trojan, continued into 09/26/2017, 09/27/2016	Attachment	11
9/26/2017	Malicious email campaign, morning	"INVOICE", 7z -> vbs -> locky ransomware, continued into 09/27/2017	Attachment	4388
9/26/2017	Malicious email campaign, morning	"Delivery status change", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	782
9/26/2017	Malicious email campaign, morning	"Invoice PIS<digits>", 7z -> vbs -> locky ransomware, continued into 09/27/2017	Attachment	3249
9/27/2017	Malicious email campaign, morning	"Your Invoice <digits> for user@domain Document is Ready for Signature", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	614
9/27/2017	Malicious email campaign, morning	"Scanned image from MX-2600N", 7z -> vbs -> locky ransomware, continued into 09/28/2017	Attachment	3777
9/27/2017	Malicious email campaign, morning	"Your <domain> BALANCE PAYMENT", r00 -> lokibot	Attachment	10
9/28/2017	Malicious email campaign, morning	"Emailing: Scan<digits>", 7z -> vbs -> trickbot and locky ransomware	Attachment	1875
9/28/2017	Malicious email campaign, morning	"Scan Data", 7z -> vbs -> locky ransomware, continued into 09/28/2017	Attachment	3542
9/28/2017	Malicious email campaign, morning	"RE: invoice <digits> debit", link -> doc -> hancitor -> pony -> evilpony -> zloader trojans	Link	272
9/29/2017	Malicious email campaign, morning	"Invoice", 7z -> vbs -> locky ransomware	Attachment	4074

Graphic courtesy of @james_inthe_box

THE CRIMEWARE ECOSYSTEM

LOCKY AND CERBER

CUSTOMER SERVICE!
Thanks CERBER… so thoughtful ;)



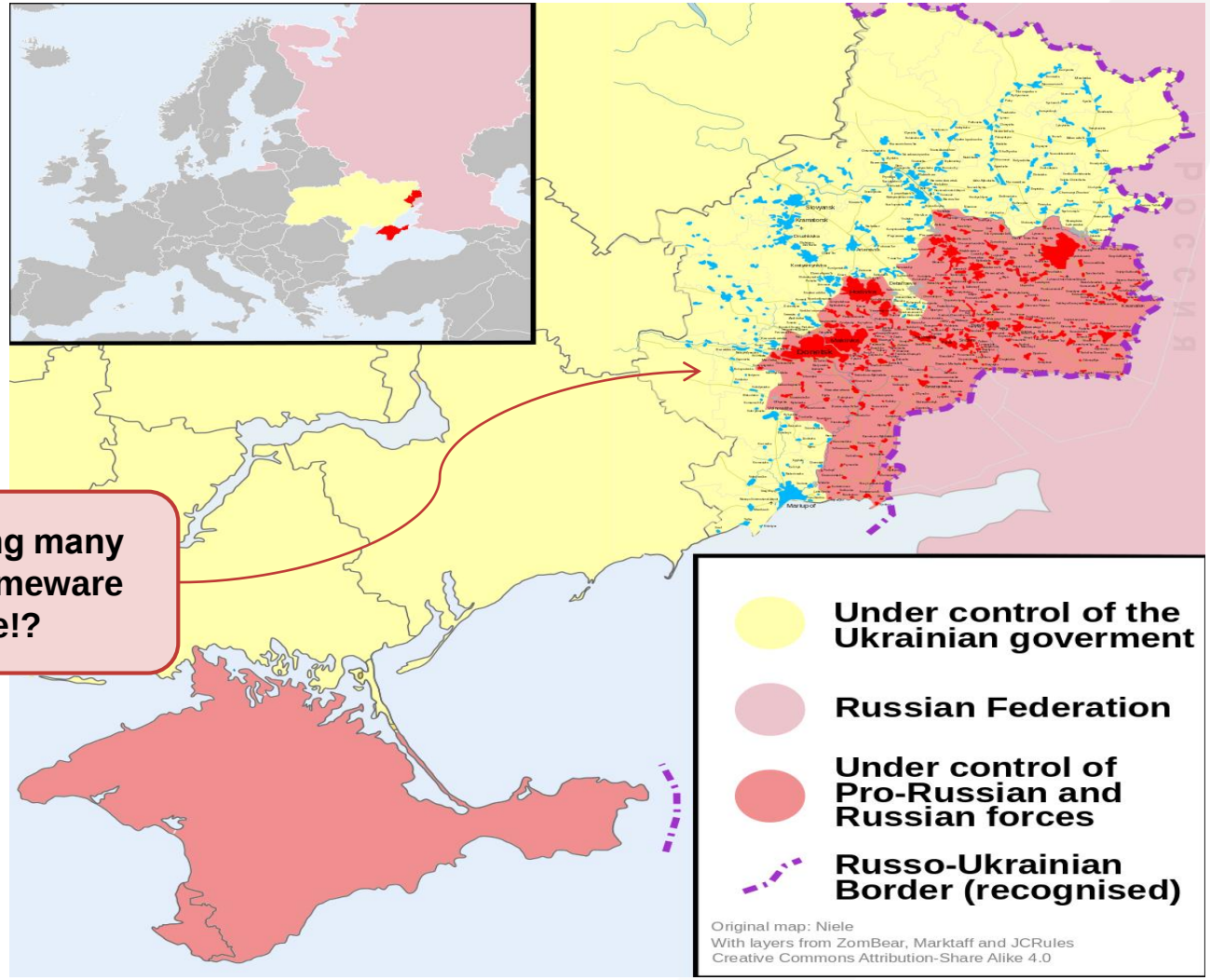
Ransomware remains a RELIABLE REVENEUE STREAM

Backup routinely & use DMARC people!

CRIMEWARE TRENDS

THE DESTABILIZATION OF UKRAINE… BULLETPROOF HOSTING?

Hey, they're not enforcing many laws… let's host our Crimeware campaign over here!?



Graphic courtesy of wikipedia

CRIMEWARE TRENDS

CREDENTIAL & INFRASTRUCTURE HARVESTING

- Continued trend for heightened rate of scanning and brute force attacks
- One of many conveniently available and botnet enabled hacking services

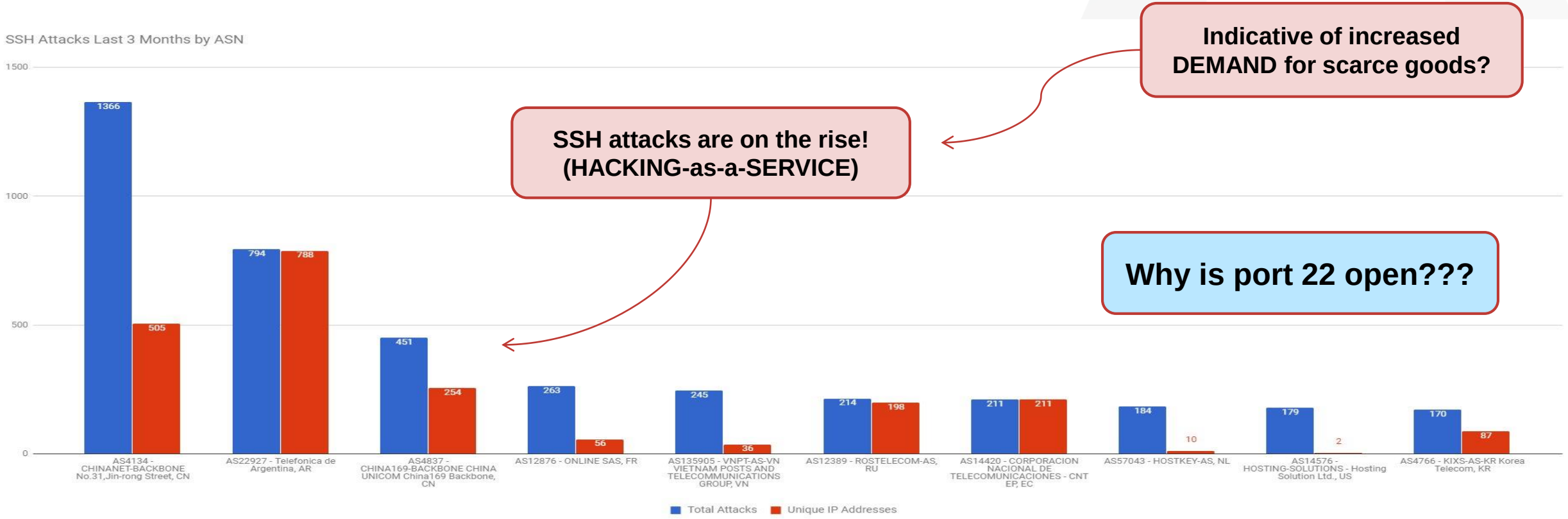
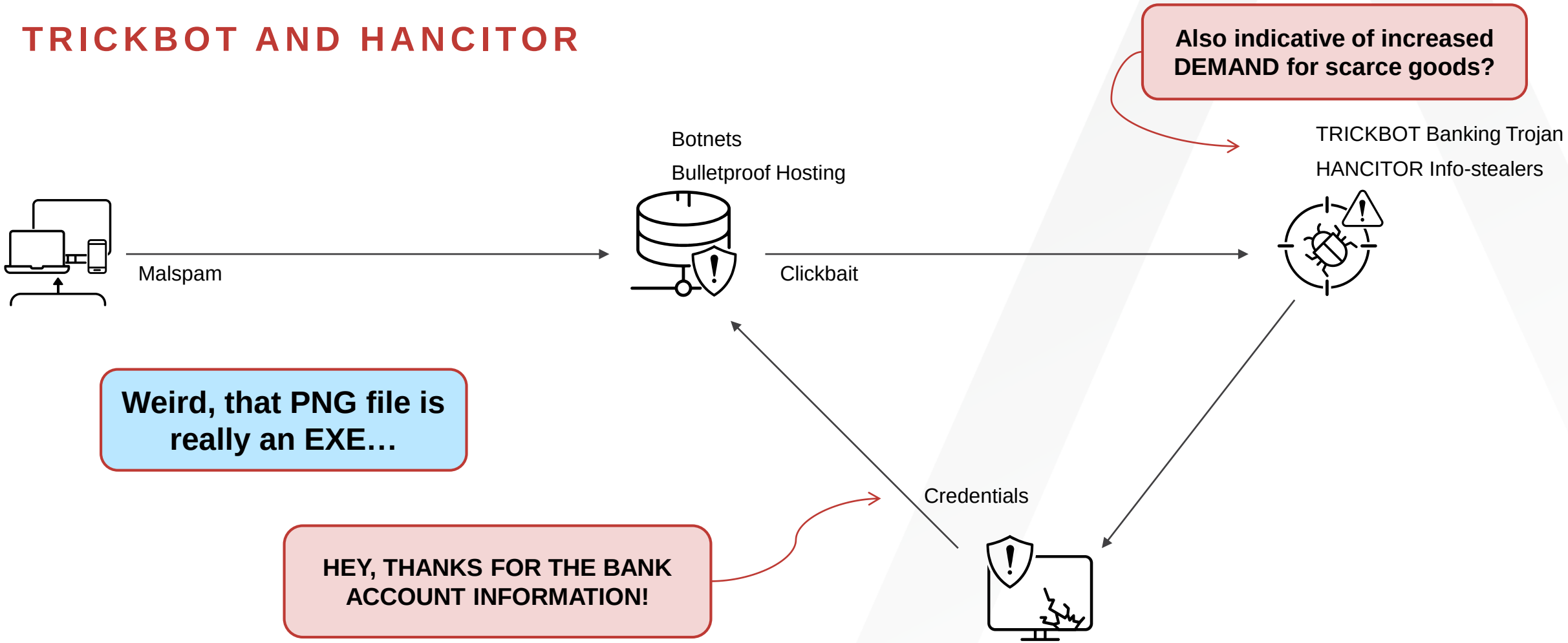


Chart credit: @bad_packets

THE CRIMEWARE ECOSYSTEM

TRICKBOT AND HANCITOR



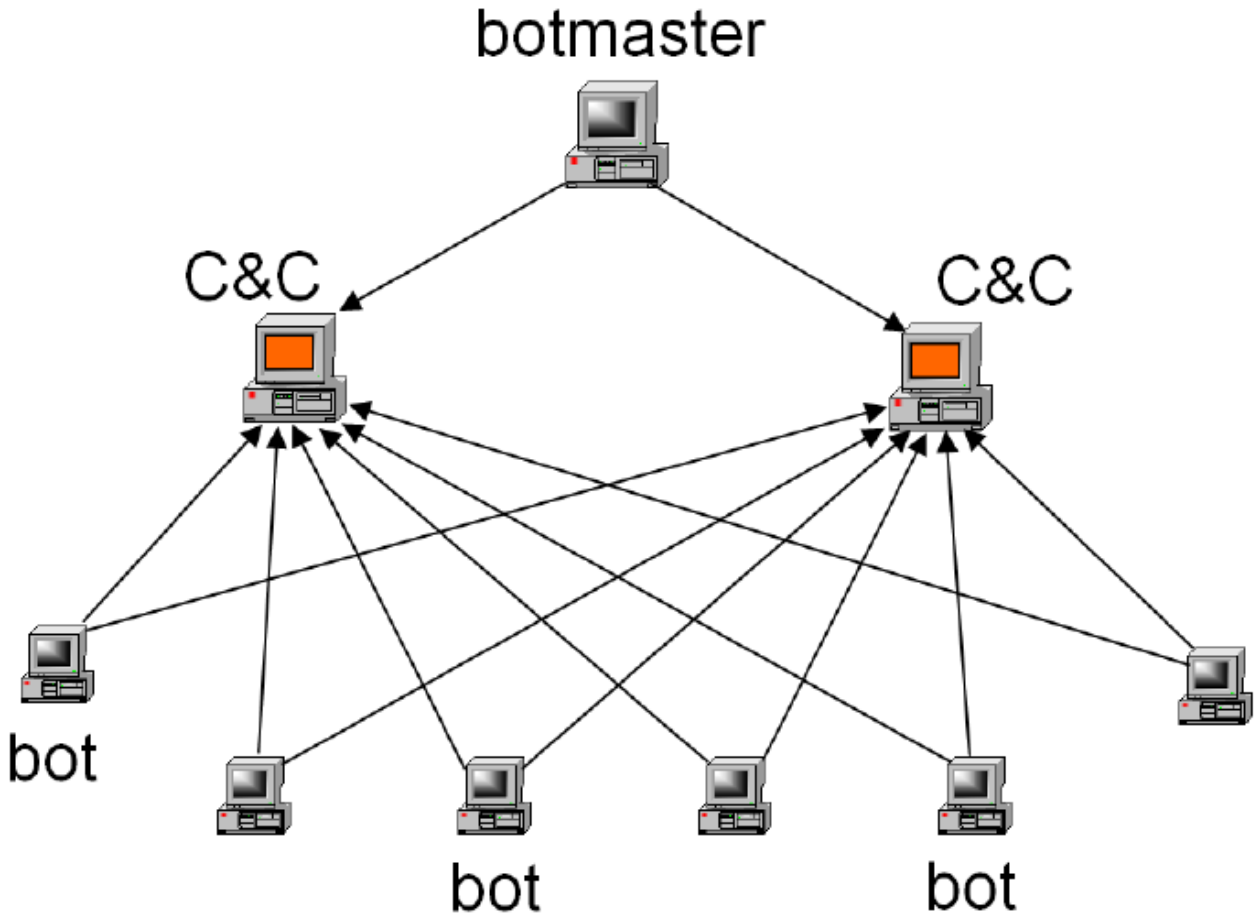
CRIMEWARE TRENDS

BOTNETS

- Current Threats
  - NECURS
    - Mixed personal computers, servers, other devices…
  - MIRAI/PERSAI
    - Internet of Things (IoT) devices
  - REAPER
    - IoT devices
  - SCHOOLBELL
    - Schools, Libraries, and more

- Just who controls these capabilities?

- How are they being weaponized?
  - Malspam (e.g., Locky)
  - Malvertising (e.g., Methbot)
  - Hacking services (e.g., DDoS)
  - Operational Relay Botnet (ORB)



CRIMEWARE TRENDS

THE DDOS THREAT

INFRASTRUCTURE INVESTMENT: DDoS now comes with pulse wave attacks to to increase your attack surface!!

- Distributed Denial of Service (DDoS)

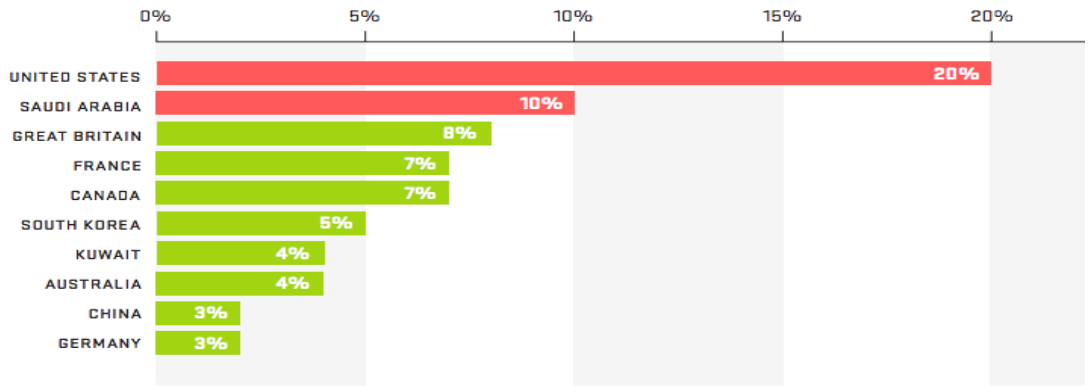


Figure AT9 *Top Targeted Countries for DDoS Attacks Greater Than 10 Gbps by Percentage*

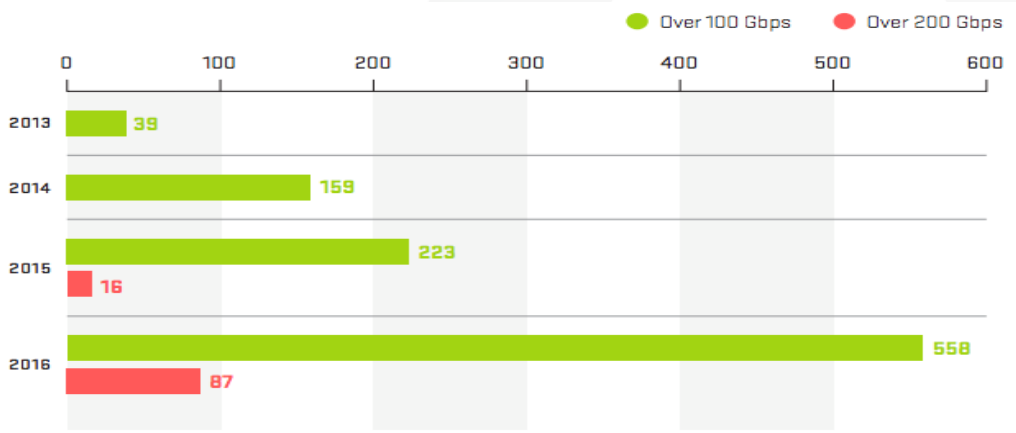


Figure AT2 *Growth in Large Attacks Year Over Year*

- DDoS Extortion

```
Hello, <obfuscated recipient>
FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!
We are Phantom Squad
Your network will be DDoS-ed starting Sept 30st 2017 if you don't pay protection fee - 0.2 Bitcoin @ 1PsjarSs9kYcBd1vCKFVAqmhDfN1vehyNZ.
If you don't pay by Sept 30st 2017, attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.
This is not a joke.
```

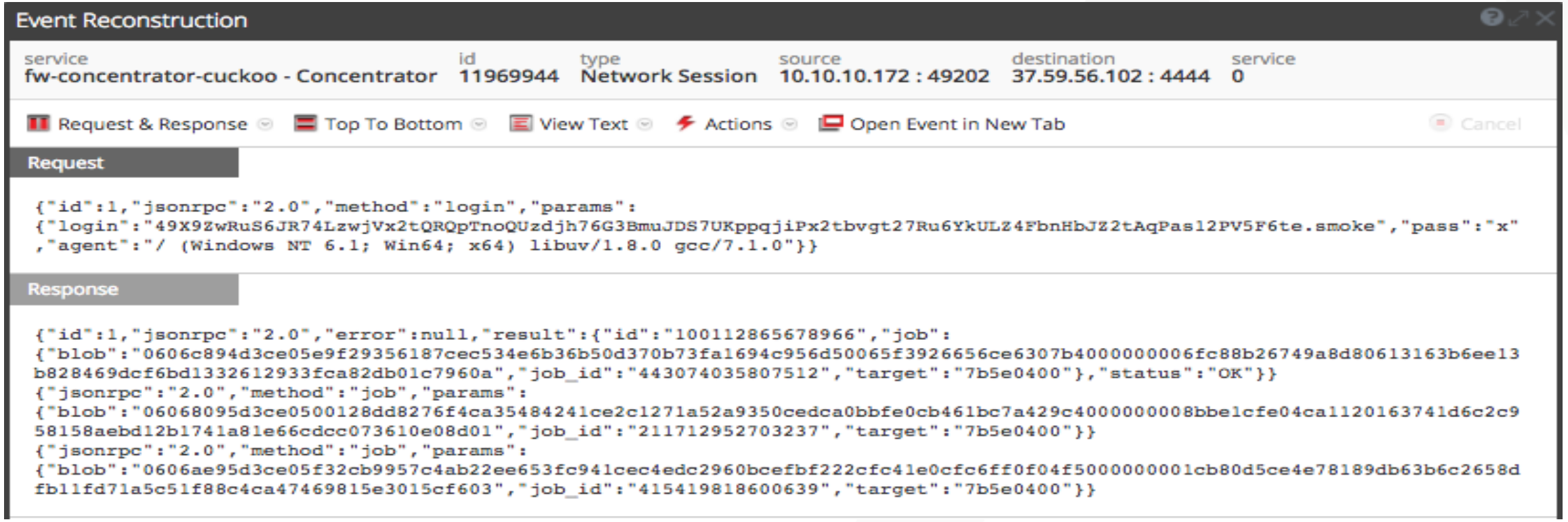
DDoS Protection & Fallback Comms Plan

Arbor Networks 12th Worldwide Infrastructure Security Report: https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf
Help Net Security: https://www.helpnetsecurity.com/2017/09/25/large-ddos-attacks/

CRIMEWARE TRENDS

RISE OF THE MINERS

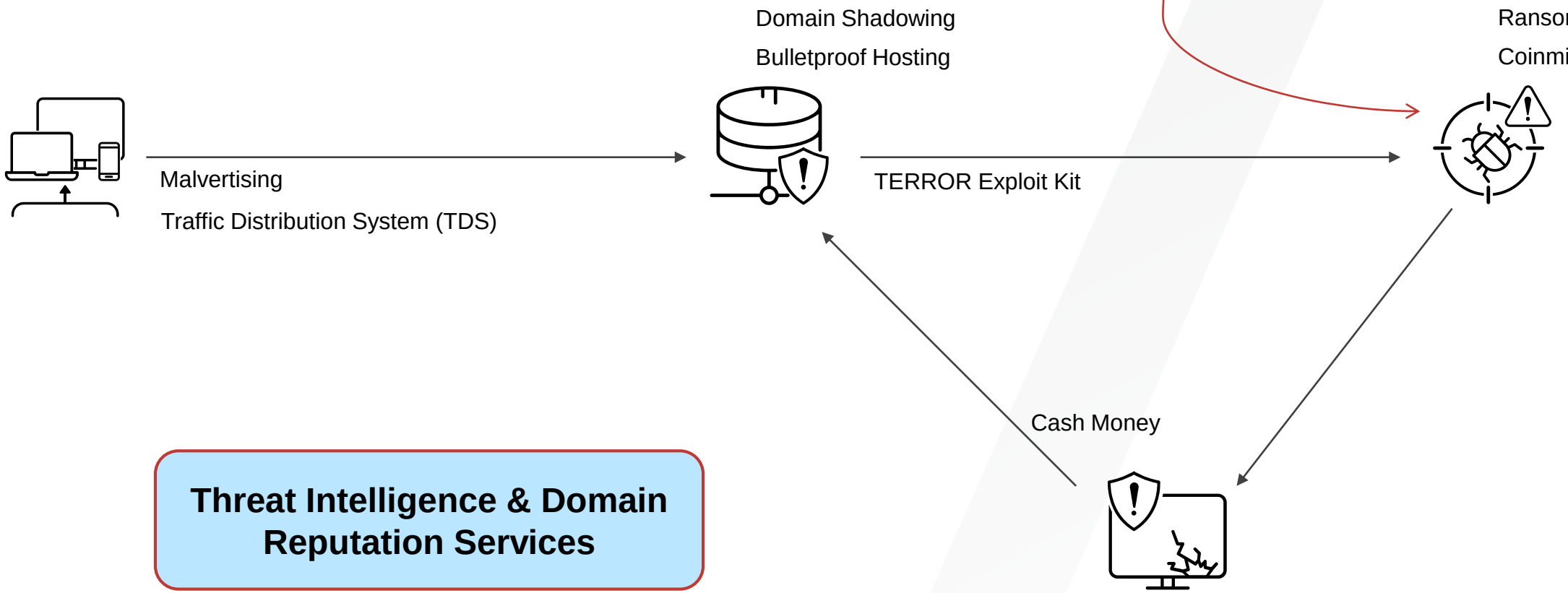
- The idea of a mathematically secure chain of blocks began in 1991 and was first conceptualized as digital currency in 1998 as ‘Bit Gold’. Bitcoin was the first decentralized digital currency and was implemented in 2009.



THE CRIMEWARE ECOSYSTEM

TERROR EXPLOIT KIT

NEW REVENUE STREAM: Mining malware and Drive-by-mining represent CAPITAL innovation by threat actors

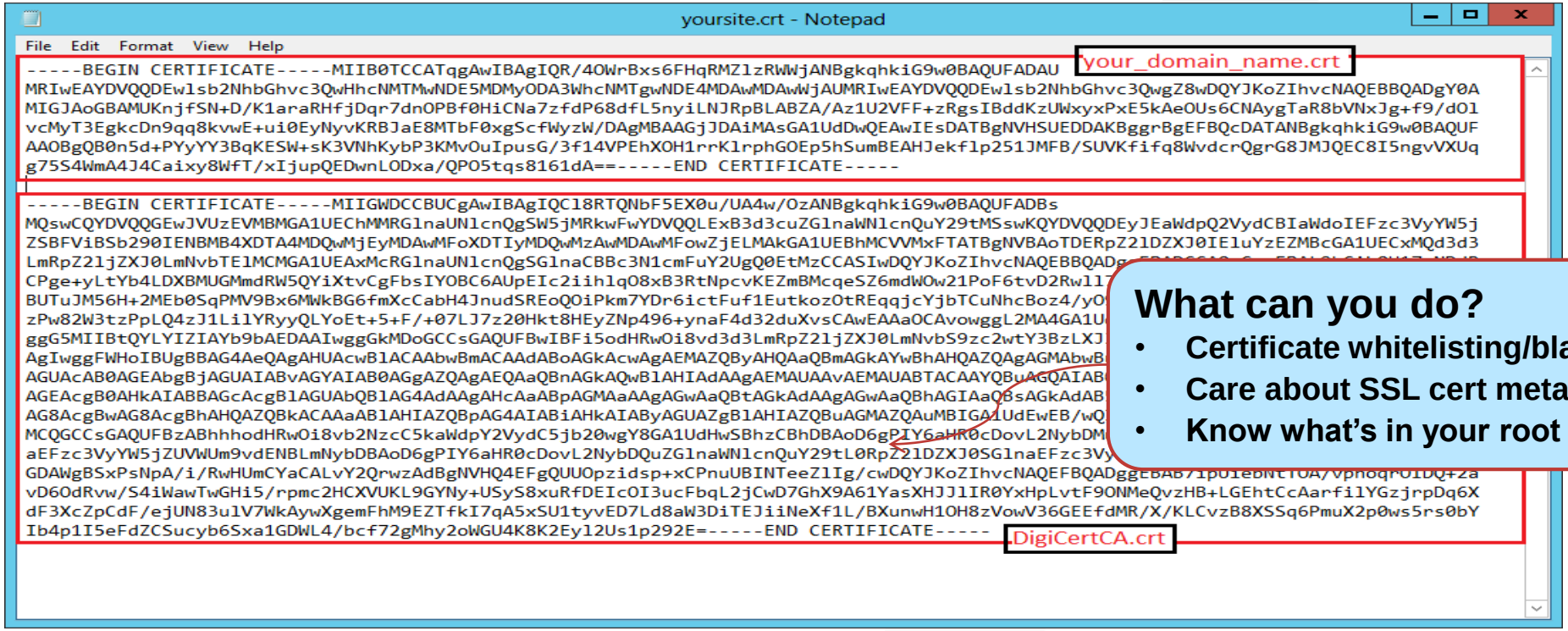


Threat Intelligence & Domain Reputation Services

CRIMEWARE TRENDS

PREVALENCE OF SSL AND CODE-SIGNING CERTS

- This trend speaks to the growing complexity of not just advanced persistent threat (APT) but also crimeware actors, and directly adds to the mounting challenges faced by defenders, who now increasingly encounter signed malware and encrypted malicious traffic.



'Borrowing Microsoft Code Signing Certificates': **https://blog.conscioushacker.io/index.php/2017/09/27/borrowing-microsoft-code-signing-certificates/**
'Subverting Trust in Windows – A Case Study of the "How" and "Why" of Engaging in Security Research': https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf

CRIMEWARE TRENDS

MOVING FORWARD

1. MALVERTISING AND MALSPAM REMAIN PRIMARY DELIVERY VECTORS
2. 'DARKNET' ISN'T GOING AWAY & EMPHASIS ON CREDENTIAL HARVESTING PERSISTS
3. RANSOMWARE & CRYPTO-CURRENCY ARE IMPORTANT REVENUE STREAMS
4. BOTNET CAPABILITIES AND BULLETPROOF HOSTING PROVIDERS INCREASE
5. INCREASED ADOPTION OF ENCRYPTION WILL BRING MORE COMPLEXITY TO DEFENDING NETWORKS

RSA

THANK YOU