Secureworks®

Ransomware Threat Briefing

Noel Reynolds – Security Engineer

March 16, 2022

Your organization’s worst day…

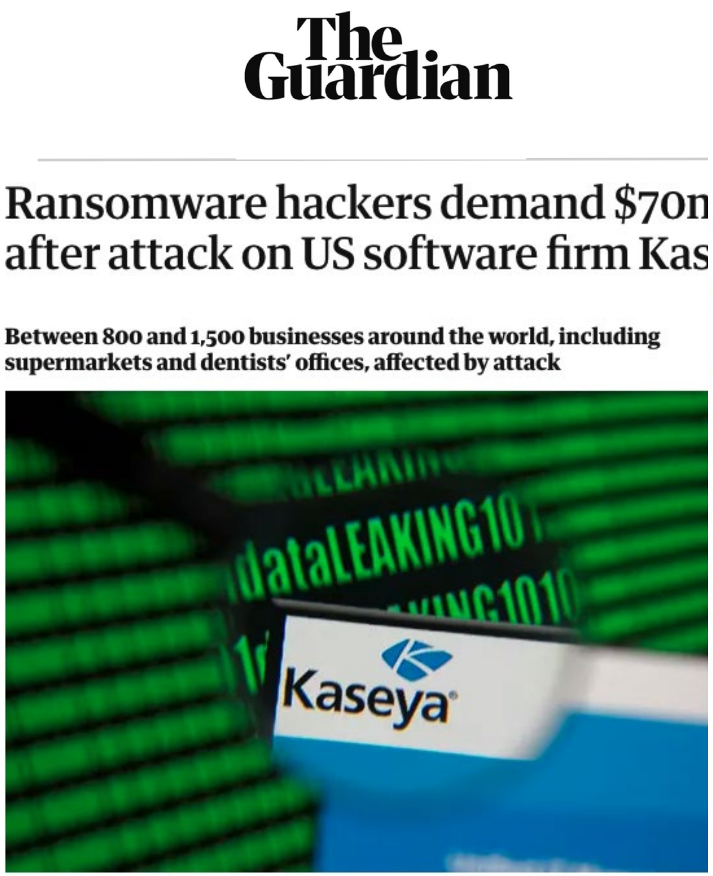
“Hello [victim company redacted]. We are Conti Group. We want to inform that your company local network have been hacked and encrypted. We downloaded from your network more than 180GB of sensitive data. – Shared HR – Shared_Accounting – Corporate Debt – Departments. You can see your page in the our blog here [dark web link]. Your page is hidden. But it will be published if you do not go to the negotiations.”

Why talk about ransomware?

- The ransomware threat landscape is active and thriving.
- Our customers continue to get hit by it.
- Other organizations continue to get hit by it.
  - Our customers want to know what happened, are they protected.
- The landscape is shifting – we don’t know how much yet.
  - Colonial Pipeline – a watershed moment?
  - Intensifying government/law enforcement response?
- We should continue to be actively looking at opportunities to prevent, detect.

Ransomware: Impossible to ignore

Opportunistic, financially motivated, highly lucrative

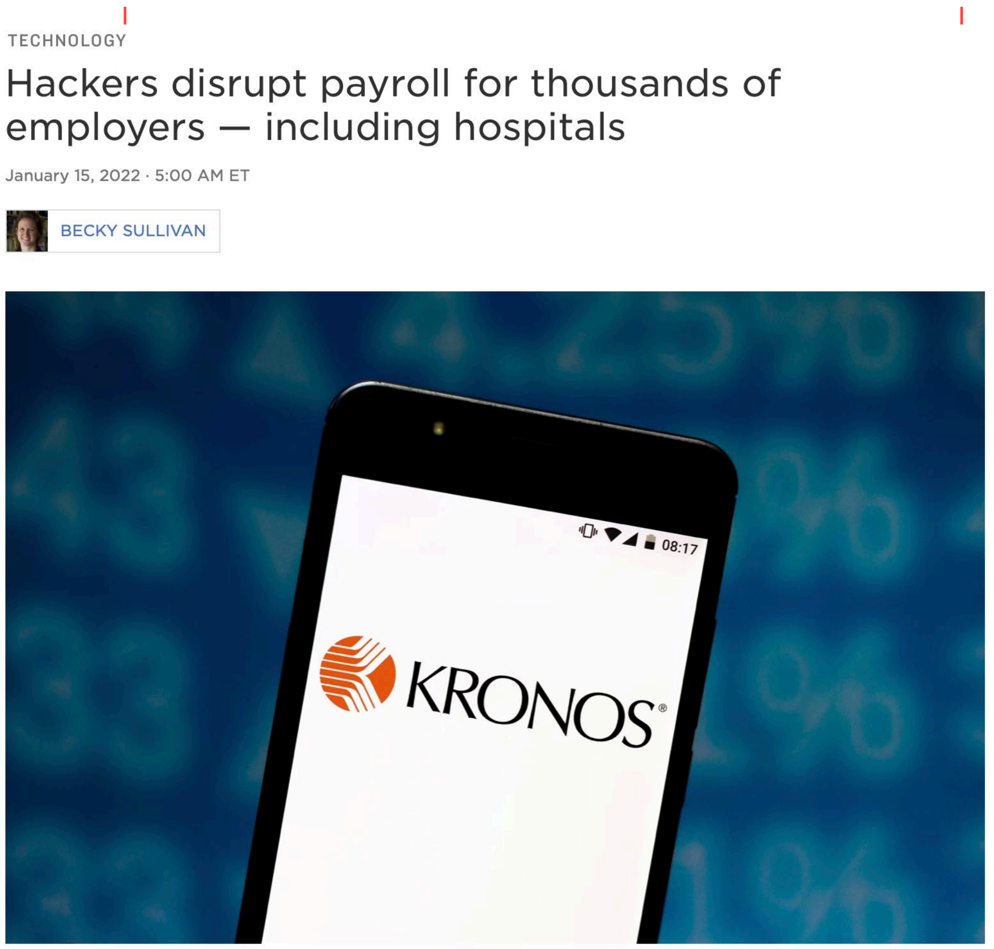


The Guardian

Ransomware hackers demand $70m after attack on US software firm Kas

Between 800 and 1,500 businesses around the world, including supermarkets and dentists' offices, affected by attack

https://www.theguardian.com/technology/2021/jul/06/kas ransomware-hackers-attack



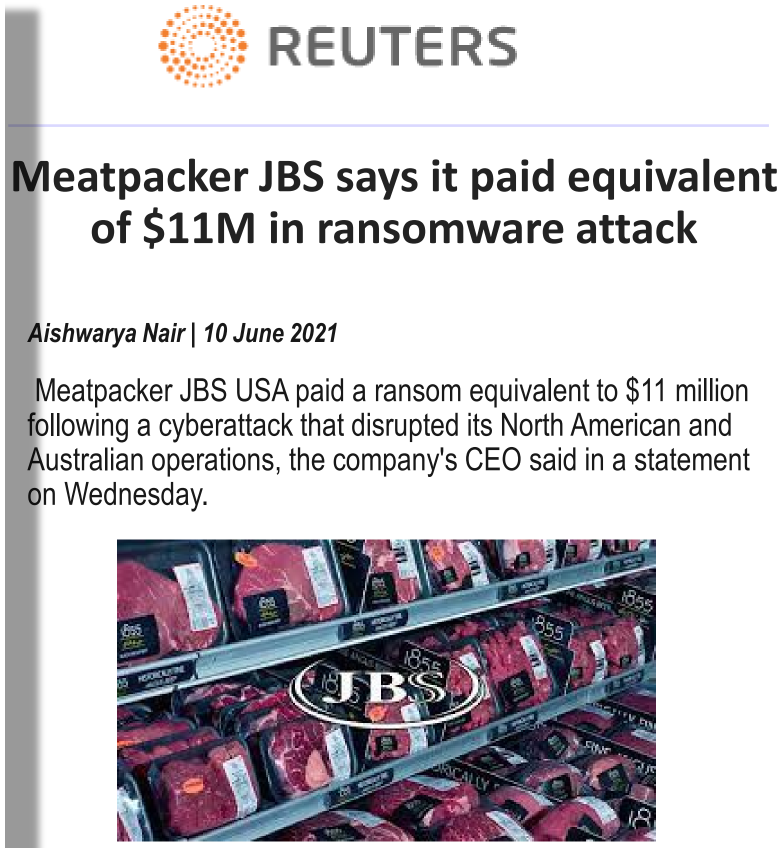
TECHNOLOGY

Hackers disrupt payroll for thousands of employers — including hospitals

January 15, 2022 · 5:00 AM ET

BECKY SULLIVAN

ransomware.html



REUTERS

Meatpacker JBS says it paid equivalent of $11M in ransomware attack

Aishwarya Nair | 10 June 2021

Meatpacker JBS USA paid a ransom equivalent to $11 million following a cyberattack that disrupted its North American and Australian operations, the company's CEO said in a statement on Wednesday.

https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/

State of the landscape

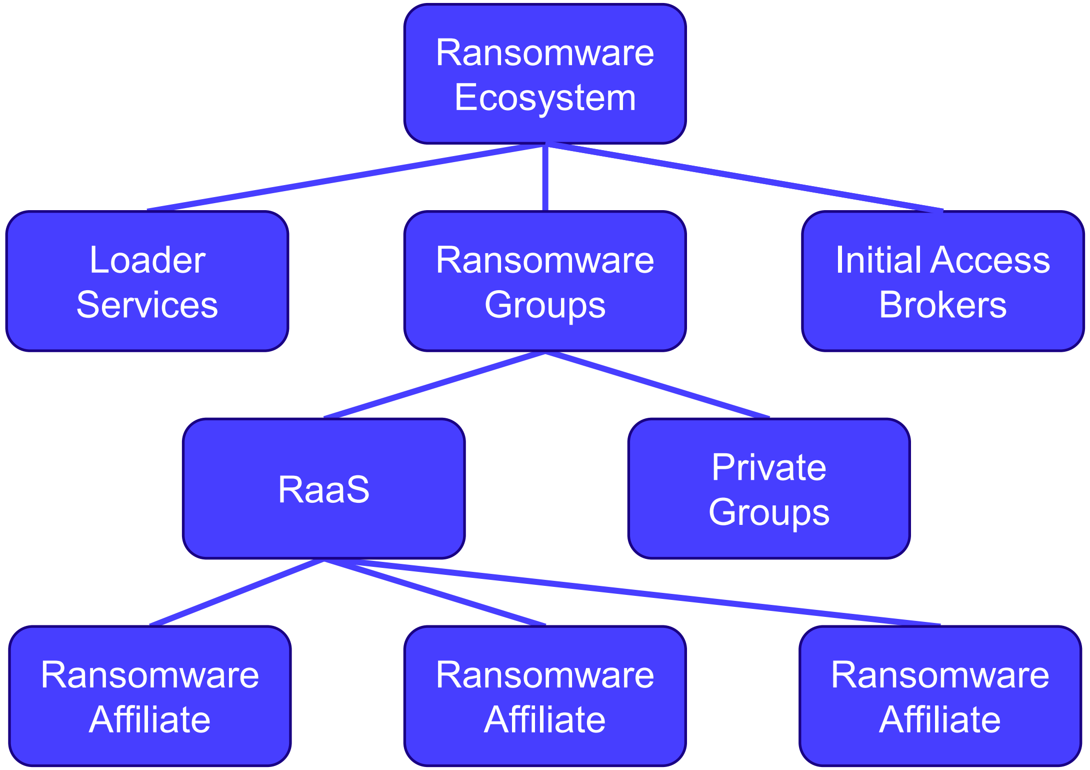
By numbers

11+	‘Ransomware-as-a-Service’ (RaaS) operations
30+	Active name-and-shame groups
2300+	Public victims (tip of the iceberg)
$40M	Highest reported public ransomware payment

A global criminal underground economy

E-crime at scale

- When we look at the Cyber Threat Landscape what we really see is a global underground economy that functions as a near peer competitor to all our customers.
- E-criminal networks, are in pursuit of the fastest path to monetization with the use of weaponized software.
- The underground economy has SAAS, PAAS and IAAS, producers, wholesalers, retailers and even venture capitalist, all aggressively pursuing **the economic goal of stealing your hard work** and productivity.

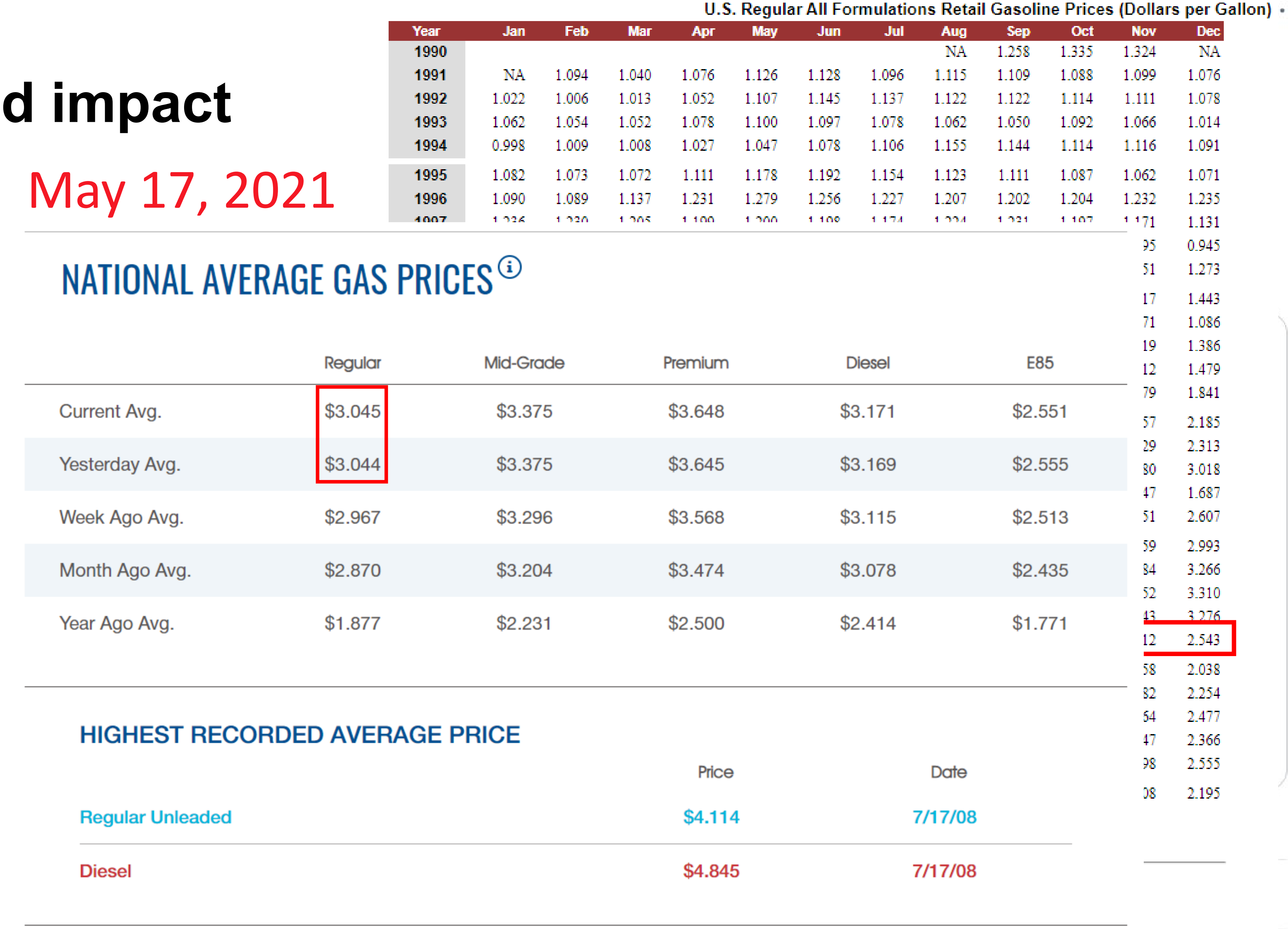


Secureworks®

Real world impact

The ‘so what’

May 17, 2021



U.S. Regular All Formulations Retail Gasoline Prices (Dollars per Gallon)

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
1990								NA	1.258	1.335	1.324	NA
1991	NA	1.094	1.040	1.076	1.126	1.128	1.096	1.115	1.109	1.088	1.099	1.076
1992	1.022	1.006	1.013	1.052	1.107	1.145	1.137	1.122	1.122	1.114	1.111	1.078
1993	1.062	1.054	1.052	1.078	1.100	1.097	1.078	1.062	1.050	1.092	1.066	1.014
1994	0.998	1.009	1.008	1.027	1.047	1.078	1.106	1.155	1.144	1.114	1.116	1.091
1995	1.082	1.073	1.072	1.111	1.178	1.192	1.154	1.123	1.111	1.087	1.062	1.071
1996	1.090	1.089	1.137	1.231	1.279	1.256	1.227	1.207	1.202	1.204	1.232	1.235
1997	1.236	1.230	1.205	1.199	1.200	1.198	1.174	1.224	1.231	1.197	1.171	1.131
											95	0.945
											51	1.273
											17	1.443
											71	1.086
											19	1.386
											12	1.479
											79	1.841
											57	2.185
											29	2.313
											80	3.018
											47	1.687
											51	2.607
											59	2.993
											84	3.266
											52	3.310
											43	3.276
											12	2.543
											58	2.038
											82	2.254
											54	2.477
											47	2.366
											98	2.555
											08	2.195

NATIONAL AVERAGE GAS PRICES ⓘ

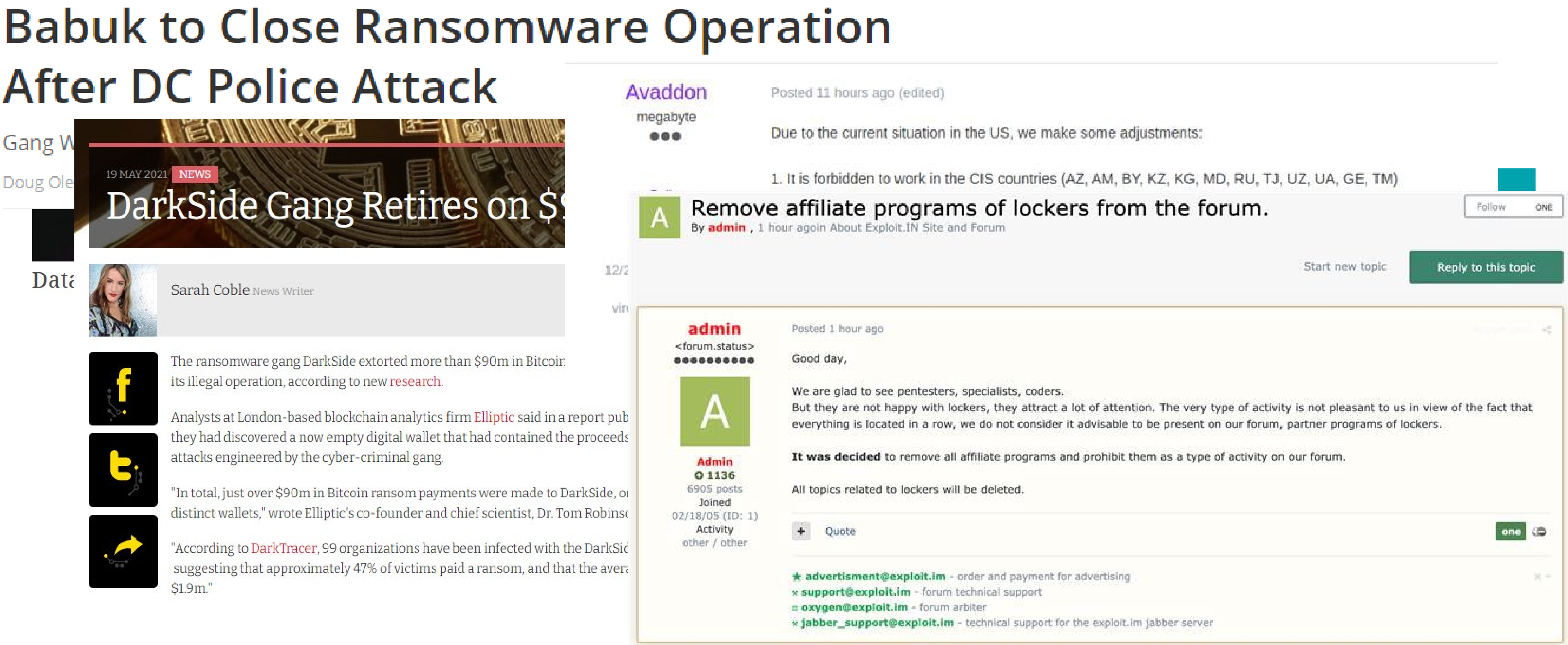
	Regular	Mid-Grade	Premium	Diesel	E85
Current Avg.	$3.045	$3.375	$3.648	$3.171	$2.551
Yesterday Avg.	$3.044	$3.375	$3.645	$3.169	$2.555
Week Ago Avg.	$2.967	$3.296	$3.568	$3.115	$2.513
Month Ago Avg.	$2.870	$3.204	$3.474	$3.078	$2.435
Year Ago Avg.	$1.877	$2.231	$2.500	$2.414	$1.771

HIGHEST RECORDED AVERAGE PRICE

	Price	Date
Regular Unleaded	$4.114	7/17/08
Diesel	$4.845	7/17/08

Dialling it back a little?

Just some re-branding, not a major re-think



Babuk to Close Ransomware Operation After DC Police Attack

Gang W

Doug Ole

Data

19 MAY 2021 NEWS

DarkSide Gang Retires on $

Sarah Coble News Writer

The ransomware gang DarkSide extorted more than $90m in Bitcoin its illegal operation, according to new research.

Analysts at London-based blockchain analytics firm Elliptic said in a report pub they had discovered a now empty digital wallet that had contained the proceeds attacks engineered by the cyber-criminal gang.

"In total, just over $90m in Bitcoin ransom payments were made to DarkSide, o distinct wallets," wrote Elliptic's co-founder and chief scientist, Dr. Tom Robins

"According to DarkTracer, 99 organizations have been infected with the DarkSid suggesting that approximately 47% of victims paid a ransom, and that the avera $1.9m."

Avaddon
megabyte
●●●

Posted 11 hours ago (edited)

Due to the current situation in the US, we make some adjustments:

1. It is forbidden to work in the CIS countries (AZ, AM, BY, KZ, KG, MD, RU, TJ, UZ, UA, GE, TM)

12/2

vir

Remove affiliate programs of lockers from the forum.

By admin , 1 hour agoin About Exploit.IN Site and Forum

admin
<forum.status>
●●●●●●●●●●
Admin
1136
6905 posts
Joined
02/18/05 (ID: 1)
Activity
other / other

Posted 1 hour ago

Good day,

We are glad to see pentesters, specialists, coders.
But they are not happy with lockers, they attract a lot of attention. The very type of activity is not pleasant to us in view of the fact that everything is located in a row, we do not consider it advisable to be present on our forum, partner programs of lockers.

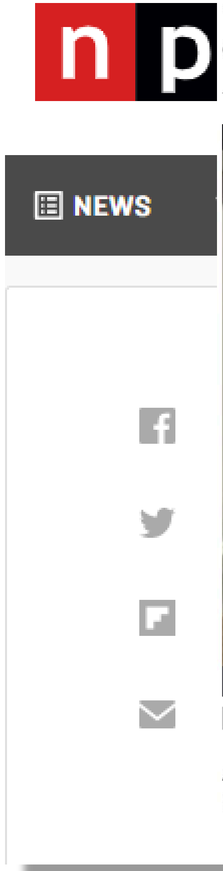
It was decided to remove all affiliate programs and prohibit them as a type of activity on our forum.

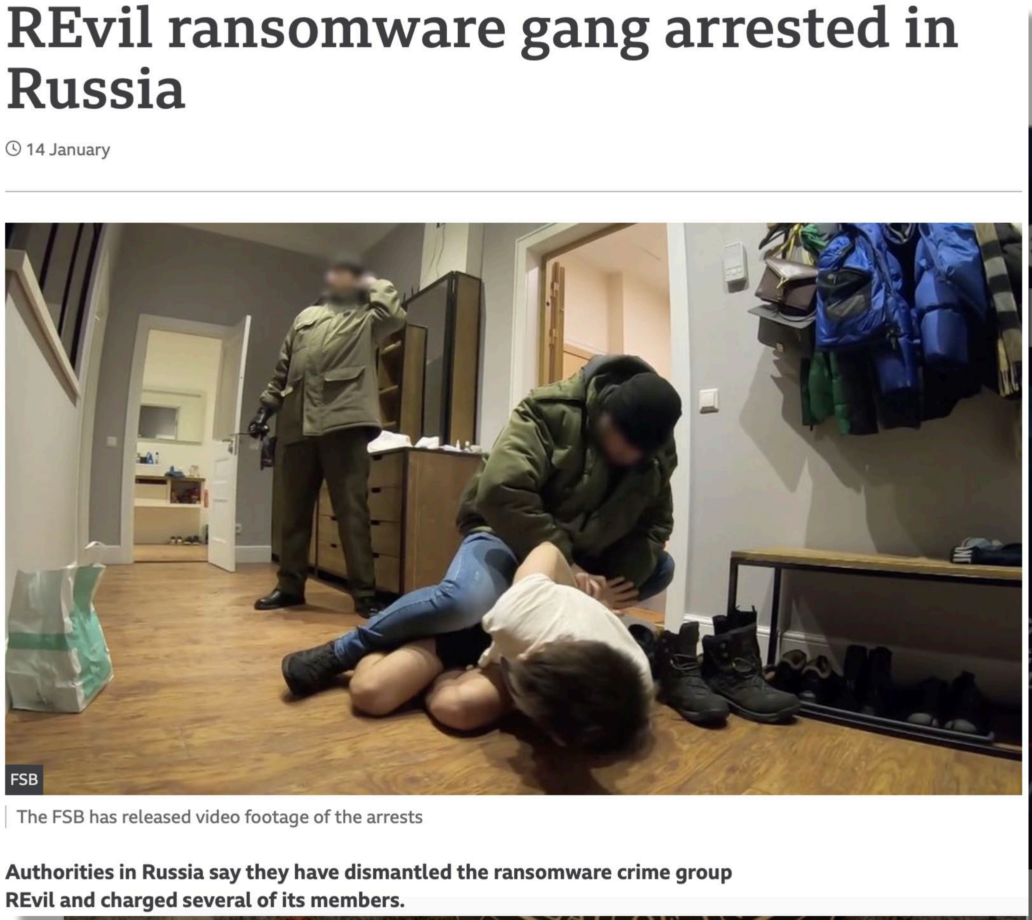
All topics related to lockers will be deleted.

★ advertisment@exploit.im - order and payment for advertising
★ support@exploit.im - forum technical support
★ oxygen@exploit.im - forum arbiter
★ jabber_support@exploit.im - technical support for the exploit.im jabber server

But we had some wins!

The greatest cat and mouse game continues





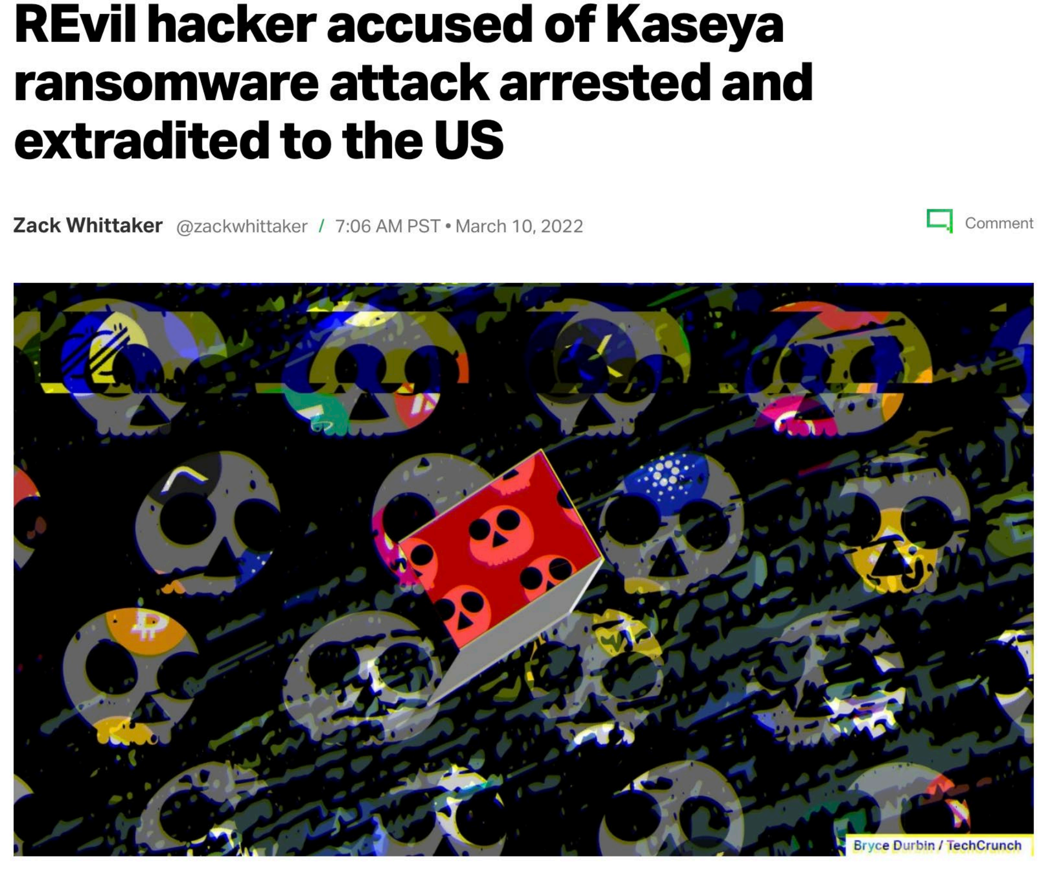
REvil ransomware gang arrested in Russia

14 January

FSB

The FSB has released video footage of the arrests

Authorities in Russia say they have dismantled the ransomware crime group REvil and charged several of its members.



REvil hacker accused of Kaseya ransomware attack arrested and extradited to the US

Zack Whittaker @zackwhittaker / 7:06 AM PST • March 10, 2022

Comment

Bryce Durbin / TechCrunch

…for the Babuk ransomware has been leaked by a threat actor on a Russian-speaking hacking forum, this week. It allows easy access to a sophisticated ransomware strain to competitors and threat actors planning to sneak into the ransomware realm with little effort.

Client impact

Second half of 2021

BUSINESS SERVICES

Snatch

EDUCATION

Dharma

FINANICAL

Cl0p
DarkSide
Makop
REvil

HEALTHCARE

WannaCry

TECHNOLOGY

RagnarLocker
Phobos

MANUFACTURING

CRING
Makop
Hades
DarkSide
Phobos
Conti

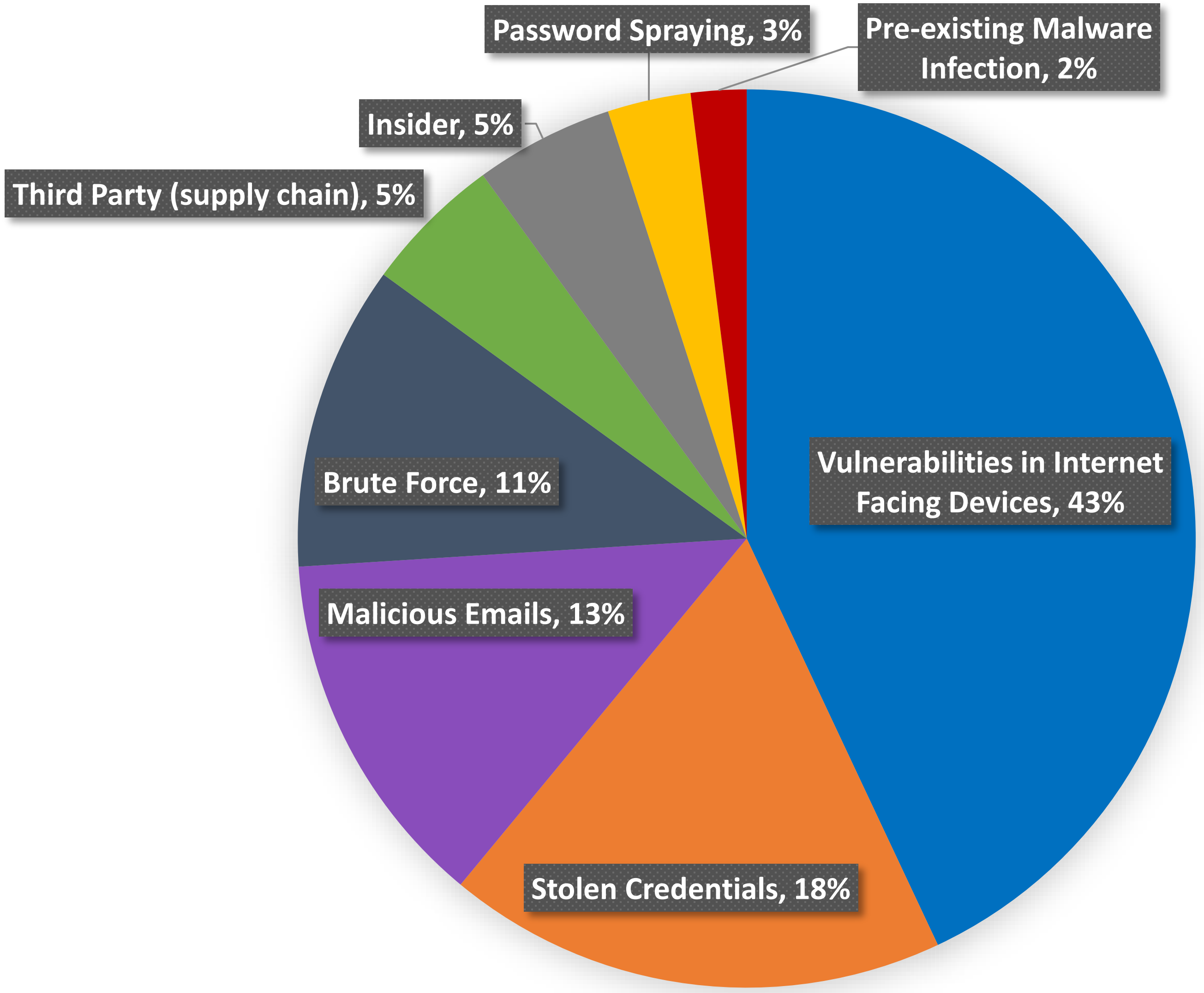
OIL & GAS

Defray

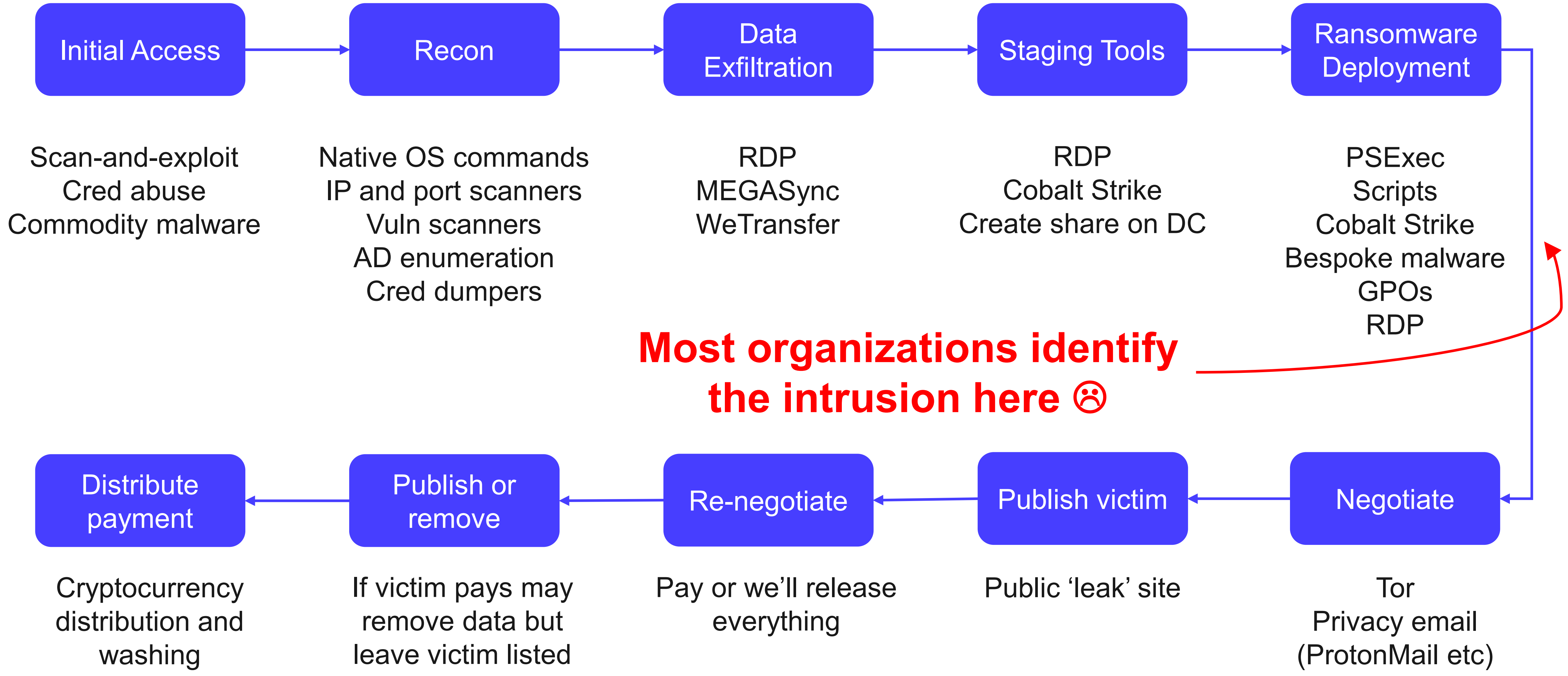
- Engagements: 41
- Greatest impact: 766 servers, 3000 workstations
- Highest ransom paid: ~$15M USD
- Shortest dwell time: 1 day
- Average dwell time: 26 days
- Longest dwell time: 303 days (ransomware not deployed)

Top Initial Access Vectors (not ransomware specific)

How are they getting in?



Anatomy of an attack



Initial Access

Scan-and-exploit
Cred abuse
Commodity malware

Recon

Native OS commands
IP and port scanners
Vuln scanners
AD enumeration
Cred dumpers

Data Exfiltration

RDP
MEGASync
WeTransfer

Staging Tools

RDP
Cobalt Strike
Create share on DC

Ransomware Deployment

PSExec
Scripts
Cobalt Strike
Bespoke malware
GPOs
RDP

Most organizations identify the intrusion here ☹

Negotiate

Tor
Privacy email
(ProtonMail etc)

Publish victim

Public ‘leak’ site

Re-negotiate

Pay or we’ll release everything

Publish or remove

If victim pays may remove data but leave victim listed

Distribute payment

Cryptocurrency distribution and washing

Are these attacks preventable?

Option 1: Prevention

Malware infection

↓

Endpoint and network detection

Scan-and-exploit

↓

Patch

Credential Abuse

↓

Multi-factor authentication

Are these attacks preventable?

Option 2: Detection and response

Good threat intel drives the right response

Effective instrumentation of the environment

Have the right people, processes and tools for rapid response

Summary

✓ #1 threat facing our customers.

✓ Indiscriminate and opportunistic.

✓ You can effectively defeat it:

- Raise the cost; make them go elsewhere.
- Not that technically sophisticated.
- Layered controls / tripwires / visibility.

✓ Many orgs pay but it’s no silver bullet.

Top 20 Specific Recommendations

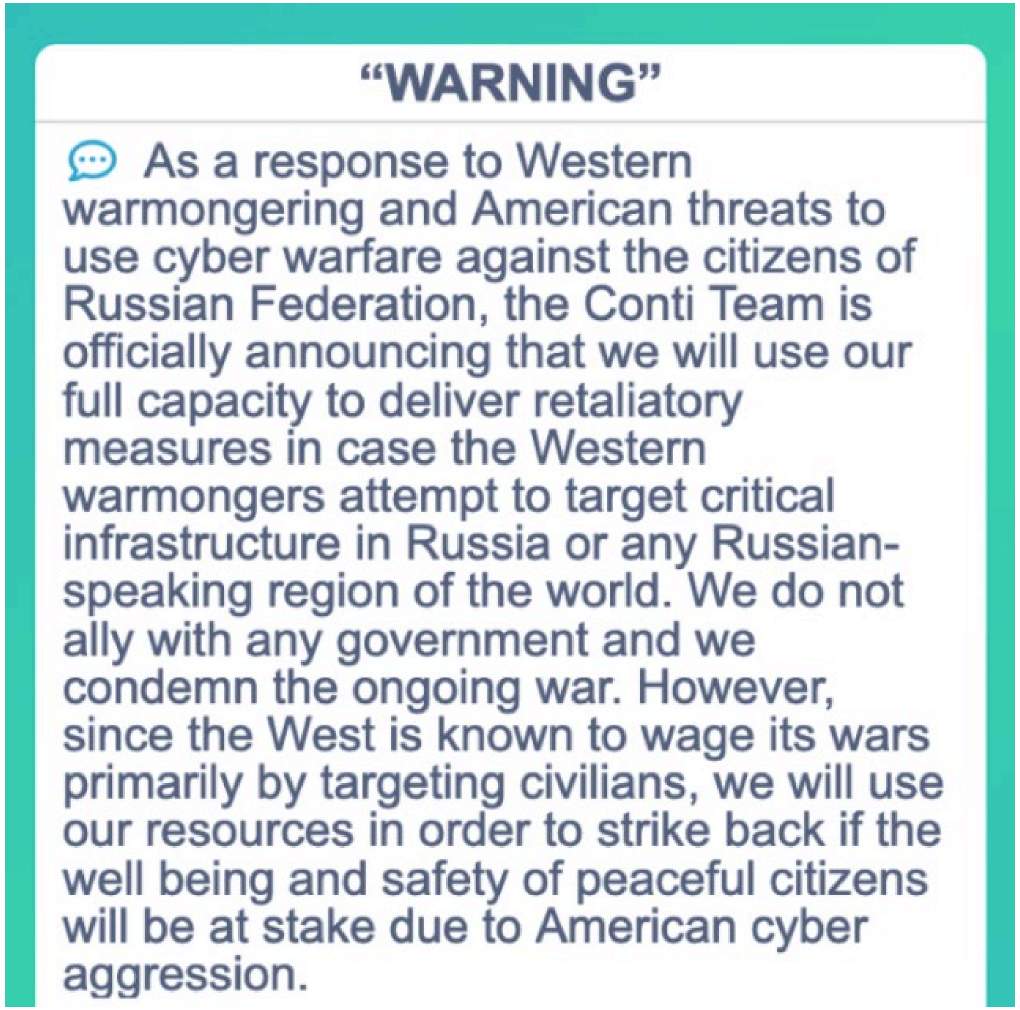
What can you do?

1. Perform regular vulnerability scans
2. Monitor for newly registered spoofed domains
3. Implement IP allow lists
4. Establish network segmentation
5. Limit mail-forwarding functionality
6. Improve backup strategy and procedures
7. Restrict USB access
8. Rebuild compromised hosts
9. Remove default/generic accounts
10. Implement multi-factor authentication
11. Implement controlled folder access
12. Audit internet-facing web systems and content
13. Block inbound RDP from the internet
14. Implement DKIM and SPF authentication
15. Implement application allow lists
16. Implement an endpoint detection and response solution
17. Block outbound FTP connections
18. Update and patch systems and software
19. Document security configurations and standards
20. Apply the principle of least-privilege to account access

Russia-Ukraine Factor

How is the war impacting the ransomware threat?

- Prior to the war, members of the ReVil ransomware gang were arrested by the Russian FSB
- Many of the Russian-led ransomware gangs appear to have Ukrainian members who are ‘flipping the table’ based on the war.
- Ukrainian security researcher provides several releases of the Conti Ransomware gang’s internal chats which tie Conti members to the Emotet botnet.



“WARNING”

💬 As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

Secureworks®