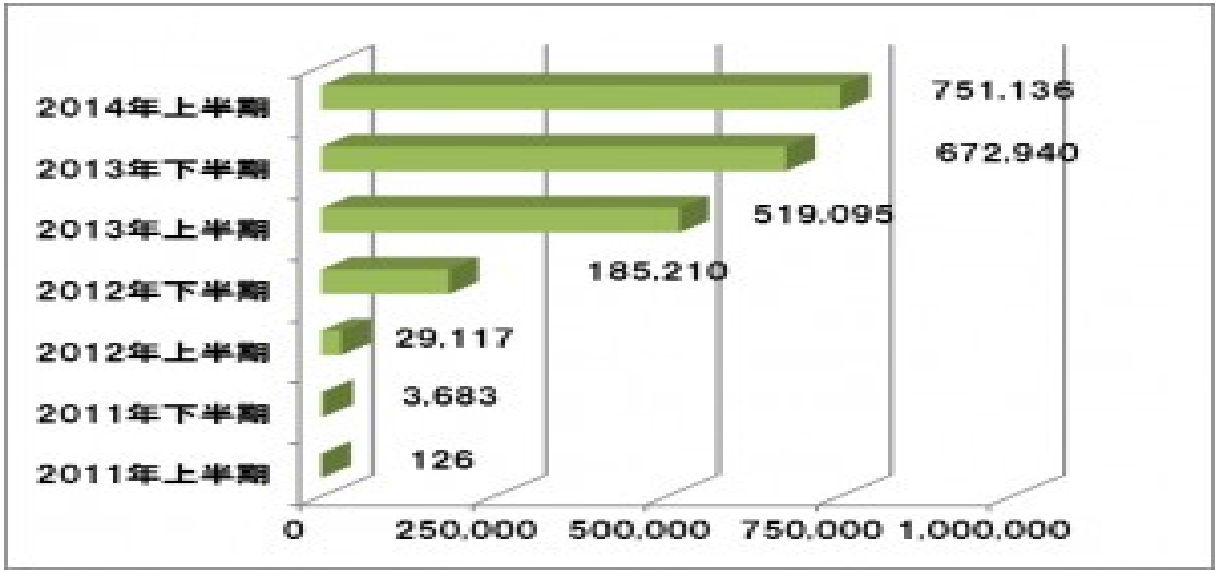
マルウェアの動作検証と Signature作成

津田塾大学学芸学部情報科学科
加藤　里奈

このテーマの目的

- 毎日世界中のどこかでマルウェアは誕生し、進化し続けている！！



出典)GDATA -2014/12/25GDATAによる
2015年マルウェア動向予測

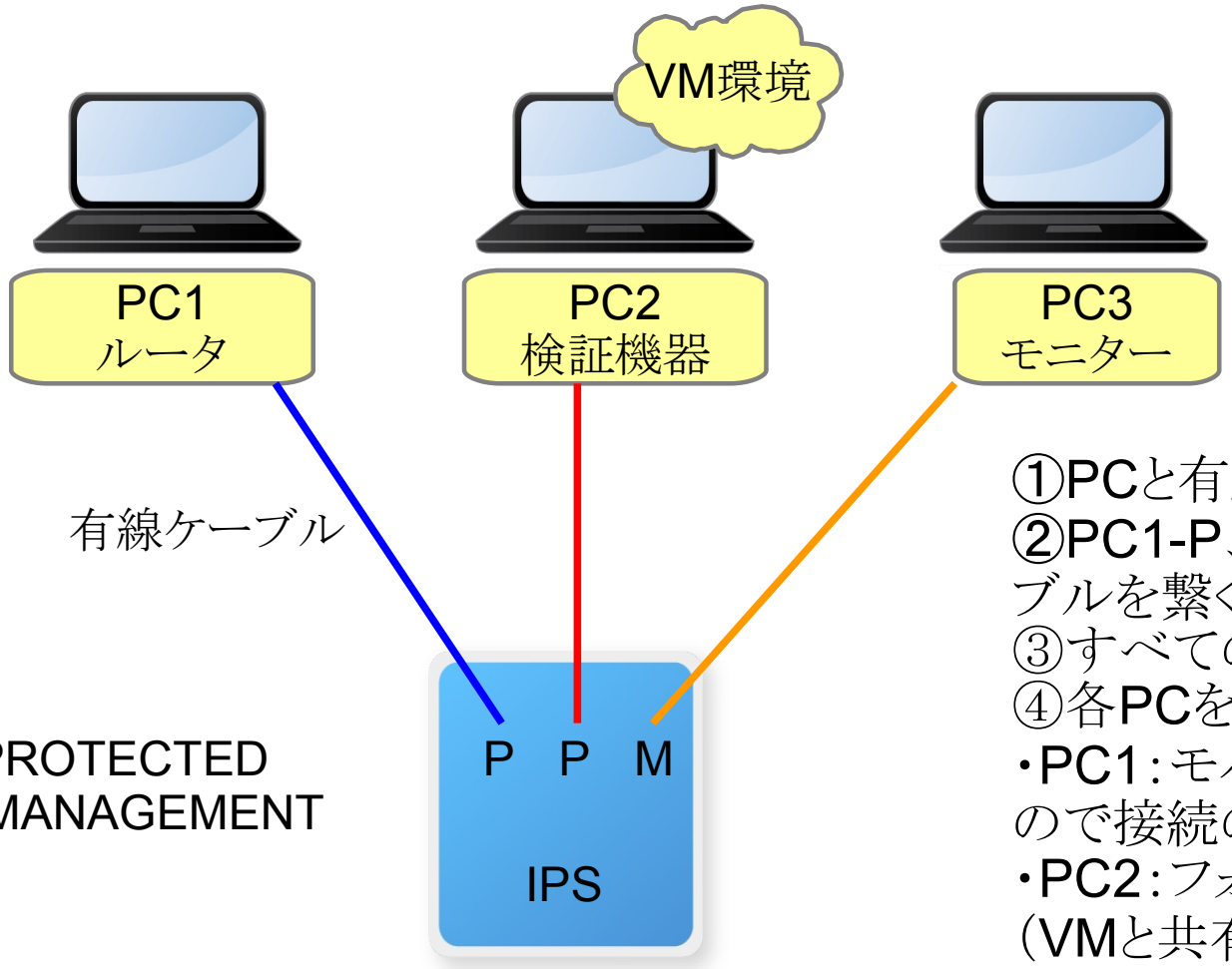
- 今のIPSでは新種のマルウェアを防ぎ切れない・・・

⇒新たなSignatureをIPSに登録して検体の通信を防ごう！

用意したもの

- PCを3台（ルーター用、検証用、モニター用）
- 有線ケーブルを3本
- IPS
- VMware
- Wireshark
- Noriben(Process Monitor)

環境構築手順



P：PROTECTED
M：MANAGEMENT

①PCと有線ケーブルを3つ用意する
②PC1-P、PC2-P、PC3-Mに有線ケーブルを繋ぐ
③すべての機器を起動させる
④各PCを設定する
・PC1：モバイルルーターに接続させるので接続の共有を許可させておく
・PC2：フォルダーを2つ作成する。（VMと共有用、ローカルで保存する用）スナップショットを作成する。
・PC3：https://192.168.50.100に接続する

検証手順

① マルウェア検体そのもの、もしくは検体のハッシュ値を用意する

② ダウンロードした検体を共有フォルダーとローカルフォルダーにコピーする

③ 事前にクリーンな状態のスナップショットになっているかを確認してVMを起動させる

④ 共有フォルダーからVM上のディスクトップへ検体をコピーする

⑤ 検体ファイル名の拡張子を「.exe」にする

⑥ Wireshark、タスクマネージャ、Noribenを起動させる（ちゃんと動いているか確認）

⑦ 検体を実行させる

⑧ ⑥で起動させて得たログを見て検体が落ち着いてきたと感じた時にログデータを保存しVMをシャットダウンさせる。

⑨ スナップショットを復元させクリーンな状態に戻す

①～⑨の繰り返し！！！

今回検証したマルウェア

- EMDIVI(RAT)・・・遠隔操作マルウェア、日本年金機構の事件で使われた
- PlugX(RAT)・・・政府機関を狙った標的型攻撃、不正な活動や情報収集を行う (2012年6月～)
- CryptWall3.0(ランサムウェア)・・・ファイルを暗号化し、暗号化したファイルを人質にお金(BitCoin)を要求
- Dridex(Banking Trojan)・・・ネットバンク不正送金マルウェア、不正なマクロが付いているドキュメントを開くと感染
- DarkKomet (RAT)・・・多数の標的型攻撃で使われたバックドア型マルウェア

15c926d2602f65be0de65fa9c06aa6c6(PlugX)

アイコン

DNSで名前解決！

Wiresharkで見た通信内容の1部

92	2015-08-17 12:36:32.175378000	192.168.137.10	8.8.8.8	DNS	86	Standard query 0x9922 A t2.ma
93	2015-08-17 12:36:32.841999000	8.8.8.8	192.168.137.10	DNS	102	Standard query response 0x9922
94	2015-08-17 12:36:33.249443000	192.168.137.10	118.193.212.98	TCP	66	49196→8080 [SYN] Seq=0 Win=819
95	2015-08-17 12:36:33.559075000	118.193.212.98	192.168.137.10	TCP	60	8080→49196 [RST, ACK] Seq=1 Ac
96	2015-08-17 12:36:34.064520000	192.168.137.10	118.193.212.98	TCP	66	[TCP Spurious Retransmission]
97	2015-08-17 12:36:34.379728000	118.193.212.98	192.168.137.10	TCP	60	8080→49196 [RST, ACK] Seq=1 Ac
98	2015-08-17 12:36:34.892366000	192.168.137.10	118.193.212.98	TCP	62	[TCP Spurious Retransmission]
99	2015-08-17 12:36:35.197390000	118.193.212.98	192.168.137.10	TCP	60	8080→49196 [RST, ACK] Seq=1 Ac

DNS通信の中身

```
⊟ Domain Name System (response)
    [Request In: 92]
    [Time: 0.666621000 seconds]
    Transaction ID: 0x9922
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ t2.mailsecurityservice.com: type A, class IN
        Name: t2.mailsecurityservice.com
        [Name Length: 26]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ t2.mailsecurityservice.com: type A, class IN, addr 118.193.212.98
        Name: t2.mailsecurityservice.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 1799
        Data length: 4
        Address: 118.193.212.98 (118.193.212.98)
```

TCP通信からUDP通信へ

120	2015-08-17 12:36:58.385334000	192.168.137.10	118.193.212.98	UDP	78	Source port: 59332 Destination port: 80
121	2015-08-17 12:36:58.385578000	192.168.137.10	118.193.212.98	UDP	78	Source port: 59332 Destination port: 80
122	2015-08-17 12:36:58.741340000	118.193.212.98	192.168.137.10	UDP	78	Source port: 8080 Destination port: 593
123	2015-08-17 12:36:58.741342000	118.193.212.98	192.168.137.10	UDP	78	Source port: 8080 Destination port: 593
124	2015-08-17 12:36:58.759806000	192.168.137.10	118.193.212.98	UDP	91	Source port: 59332 Destination port: 80
125	2015-08-17 12:36:58.916694000	192.168.137.10	118.193.212.98	UDP	52	Source port: 59332 Destination port: 80
126	2015-08-17 12:36:58.979191000	192.168.137.10	118.193.212.98	UDP	52	Source port: 59332 Destination port: 80
127	2015-08-17 12:36:59.040633000	192.168.137.10	118.193.212.98	UDP	52	Source port: 59332 Destination port: 80
128	2015-08-17 12:36:59.103121000	192.168.137.10	118.193.212.98	UDP	52	Source port: 59332 Destination port: 80
129	2015-08-17 12:36:59.166719000	192.168.137.10	118.193.212.98	UDP	52	Source port: 59332 Destination port: 80
130	2015-08-17 12:36:59.189566000	118.193.212.98	192.168.137.10	UDP	60	Source port: 8080 Destination port: 593
131	2015-08-17 12:36:59.353632000	118.193.212.98	192.168.137.10	UDP	60	Source port: 8080 Destination port: 593

モバイルルーターのISPによってTCP通信で
SYNパケット送った際にRST返したので
UDP通信に切り替えたのではないかと想定している

23d8f7a4b4668b64d5cc4c4a84edfe7d (CryptWall3.0)

アイコン

すさまじい速さで様々な
サイトの名前解決をしている

Wiresharkで見た通信の1部

44	2015-08-18 10:10:56.017293000	192.168.137.10	8.8.8.8	DNS	81	Standard query 0xc7ce A ezglobalmarketing.com
45	2015-08-18 10:10:56.211460000	8.8.8.8	192.168.137.10	DNS	97	Standard query response 0xc7ce A 199.116.252.134
46	2015-08-18 10:10:56.212535000	192.168.137.10	199.116.252.134	TCP	66	49176→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
47	2015-08-18 10:10:56.517814000	199.116.252.134	192.168.137.10	TCP	66	80→49176 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK
48	2015-08-18 10:10:56.517878000	192.168.137.10	199.116.252.134	TCP	54	49176→80 [ACK] Seq=1 Ack=1 Win=65800 Len=0
49	2015-08-18 10:10:56.518400000	192.168.137.10	199.116.252.134	HTTP	708	GET /wp-content/themes/r.php?D0B1745184D4B19325F8CA239D78E804
50	2015-08-18 10:10:56.520339000	199.116.252.134	192.168.137.10	TCP	60	80→49176 [RST] Seq=1 Win=2097152 Len=0
51	2015-08-18 10:10:56.529829000	192.168.137.10	8.8.8.8	DNS	76	Standard query 0xe409 A shmetterheath.ru
52	2015-08-18 10:10:57.335250000	8.8.8.8	192.168.137.10	DNS	92	Standard query response 0xe409 A 217.12.207.33
53	2015-08-18 10:10:57.336307000	192.168.137.10	217.12.207.33	TCP	66	49177→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
54	2015-08-18 10:10:57.745517000	217.12.207.33	192.168.137.10	TCP	66	80→49177 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK
55	2015-08-18 10:10:57.745582000	192.168.137.10	217.12.207.33	TCP	54	49177→80 [ACK] Seq=1 Ack=1 Win=65800 Len=0
56	2015-08-18 10:10:57.746024000	192.168.137.10	217.12.207.33	HTTP	671	GET /wp-content/themes/r.php?D0B1745184D4B19325F8CA239D78E804
57	2015-08-18 10:10:57.747447000	217.12.207.33	192.168.137.10	TCP	60	80→49177 [RST] Seq=1 Win=262144 Len=0

CryptoWall3.0によって出現した脅迫状

What happened to your files?
All of your files were protected by a strong encryption with RSA-2048
More information about the encryption RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program, which is on our SECRET SERVER!!!.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If for some reasons the addresses are not available, follow these steps:

If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. http://aep554w4fm8j.fflroe598qu.com/1BEFF843881829
2. http://aoei243548ld.keedo93i1lo.com/1BEFF843881829
3. https://zpr5huq4bgmutfnf.onion.to/1BEFF843881829

http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: zpr5huq4bgmutfnf.onion/1BEFF843881829
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

Your Personal PAGE: http://aep554w4fm8j.fflroe598qu.com/1BEFF843881829
Your Personal PAGE (using TOR): zpr5huq4bgmutfnf.onion/1BEFF843881829
Your personal code (if you open the site (or TOR 's) directly): 1BEFF843881829

掲載されているURLに飛んでみたら・・・

Your files are encrypted.

To get the key to decrypt files you have to pay 500 USD. If payment is not made before 01/09/15 the cost of decrypting files will increase 2 times and will be 1000 USD

Prior to increasing the amount left:

First connect IP: 49.239.78.113

Refresh | Payment | FAQ | Decrypt 1 file for FREE | Support

We are presenting a special software - CryptoWall Decrypter - which allows to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You can make payment with BitCoins, there are many methods to get them.

bitcoin

2. You should register Bitcon wallet (click here for more information with pictures)

3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- LocalBitcoins.com (WU) - Buy Bitcoins with Western Union
- Coincafe.com - **Recommended for fast, simple service. Payment Methods: Western Union, Bank of America,Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, In Person**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- btcdirect.eu - THE BEST FOR EUROPE
- coinrnr.com - Another fast way to buy bitcoins
- bitquick.co - Buy Bitcoins Instantly for Cash
- How To Buy Bitcoins - An international directory of bitcoin exchanges.
- Cash Into Coins - Bitcoin for cash.
- CoinJar - CoinJar allows direct bitcoin purchases on their site.
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

4. Send 2.3 BTC to Bitcoin address: 1Abb4YxbRGULBB6NeXrLdh8CZpNsP2Rzwt

5. Enter the Transaction ID and chose payment option:

2.3 BTC ~= 500 USD | Clear

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214efca56ef039386ddb929c40bf34f19a27c42f07f5cf3e2aa08114c4d1f2)

6. Please check the payment information and click "PAY".

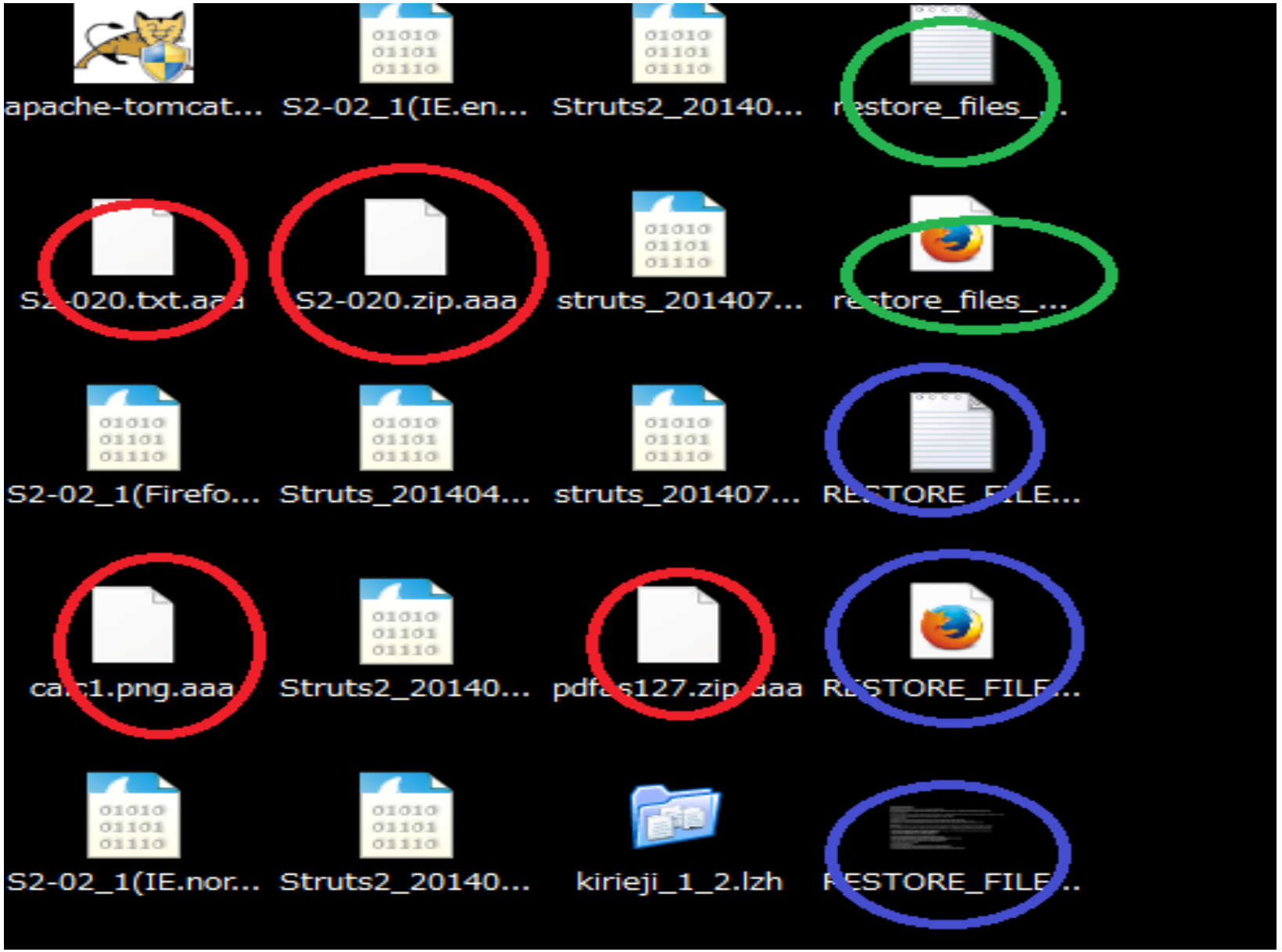
PAY

Your sent drafts

Num	Draft type	Draft number or transaction ID	Amount	Status

Your payments not found.

CryptoWall3.0起動後のデスクトップ画面



01078f660f979b30e4624e57cf986b6c (Dridex)

DNSで名前解決
していない！

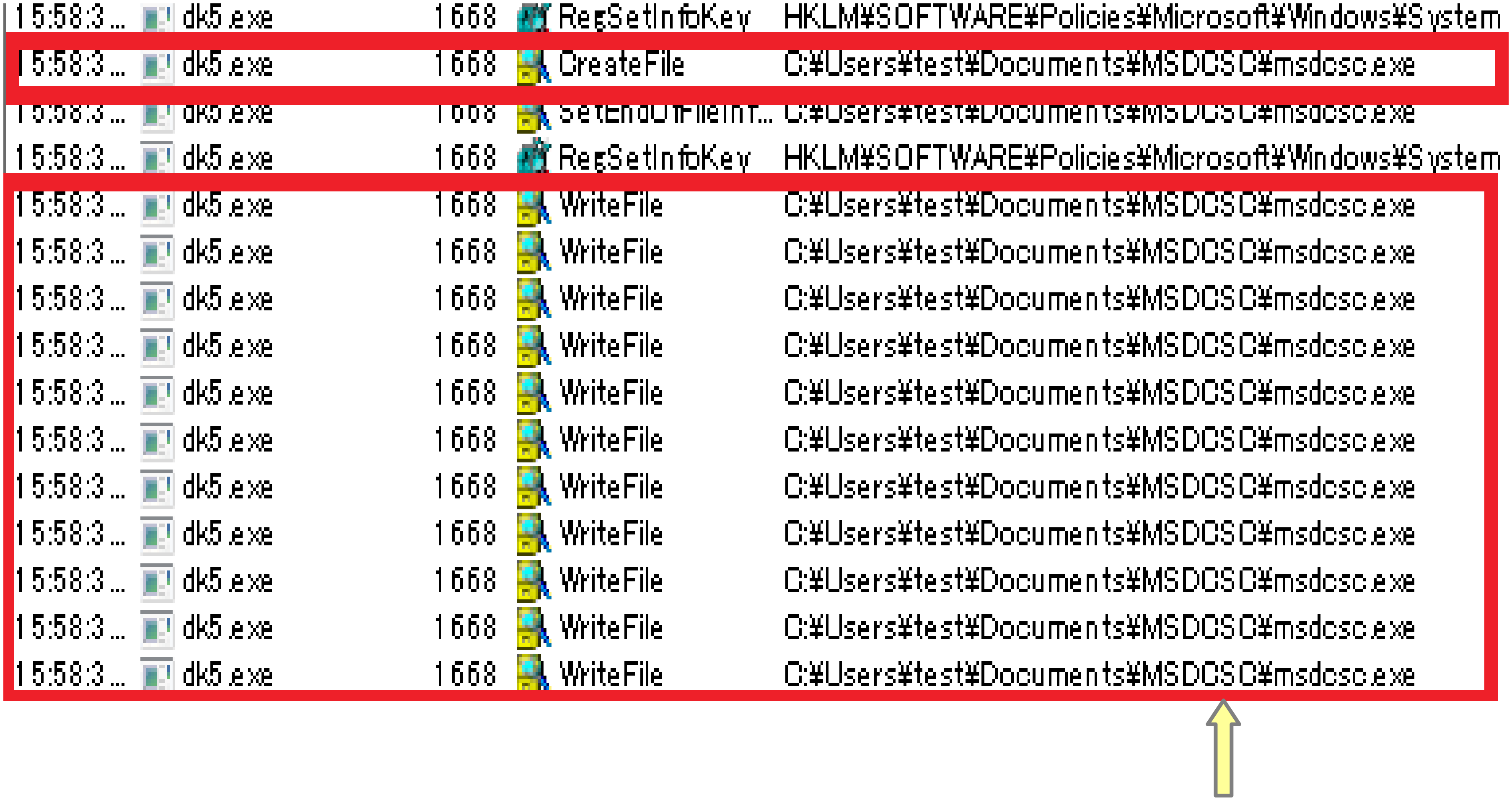
Wiresharkで見た通信の1部

9	2015-08-1[illegible]	[illegible]	[illegible]	ARP	42 192.168.137.10 is at 08:00:27:6d:1a:b2
10	2015-08-19 16:37:15.807289000	74.208.11.204	192.168.137.10	TCP	60 8080→49179 [RST, ACK] Seq=1 Ack=1 Win=0
11	2015-08-19 16:37:16.323803000	192.168.137.10	74.208.11.204	TCP	66 [TCP Spurious Retransmission] 49179→8080
12	2015-08-19 16:37:16.697337000	74.208.11.204	192.168.137.10	TCP	60 8080→49179 [RST, ACK] Seq=1 Ack=1 Win=0
13	2015-08-19 16:37:17.214111000	192.168.137.10	74.208.11.204	TCP	62 [TCP Spurious Retransmission] 49179→8080
14	2015-08-19 16:37:17.546312000	74.208.11.204	192.168.137.10	TCP	60 8080→49179 [RST, ACK] Seq=1 Ack=1 Win=0
15	2015-08-19 16:37:18.542662000	192.168.137.10	81.169.156.5	TCP	66 49180→8080 [SYN] Seq=0 Win=20480 Len=0 M
16	2015-08-19 16:37:18.978731000	81.169.156.5	192.168.137.10	TCP	60 8080→49180 [RST, ACK] Seq=1 Ack=1 Win=0
17	2015-08-19 16:37:19.183102000	192.168.137.1	192.168.137.255	DNS	158 Standard query 0x00ff
18	2015-08-19 16:37:19.494668000	192.168.137.10	81.169.156.5	TCP	66 [TCP Spurious Retransmission] 49180→8080
19	2015-08-19 16:37:19.900015000	81.169.156.5	192.168.137.10	TCP	60 8080→49180 [RST, ACK] Seq=1 Ack=1 Win=0
20	2015-08-19 16:37:20.416271000	192.168.137.10	81.169.156.5	TCP	62 [TCP Spurious Retransmission] 49180→8080
21	2015-08-19 16:37:20.821831000	81.169.156.5	192.168.137.10	TCP	60 8080→49180 [RST, ACK] Seq=1 Ack=1 Win=0
22	2015-08-19 16:37:21.807012000	192.168.137.10	74.208.11.204	TCP	66 49181→8080 [SYN] Seq=0 Win=20480 Len=0 M
23	2015-08-19 16:37:22.152186000	74.208.11.204	192.168.137.10	TCP	60 8080→49181 [RST, ACK] Seq=1 Ack=1 Win=0
24	2015-08-19 16:37:22.649915000	192.168.137.10	74.208.11.204	TCP	66 [TCP Spurious Retransmission] 49181→8080

89ef10cb2f88c5c56db1df063657249a (DarkKomet)

2015-08-20 15:58:41.137851000	192.168.137.10	8.8.8.8	DNS	88	Standard query 0x677d A nothinginteresting.zapto.org
2015-08-20 15:58:41.474436000	8.8.8.8	192.168.137.10	DNS	104	Standard query response 0x677d A 89.34.219.145
2015-08-20 15:58:41.534623000	192.168.137.10	89.34.219.145	TCP	66	49885→1604 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 S
2015-08-20 15:58:42.297058000	92.86.33.125	192.168.137.10	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit
2015-08-20 15:58:42.968279000	192.168.137.1	192.168.137.255	DNS	158	Standard query 0x00ff
2015-08-20 15:58:44.542695000	192.168.137.10	89.34.219.145	TCP	66	[TCP Retransmission] 49885→1604 [SYN] Seq=0 Win=8192 L
2015-08-20 15:58:44.847977000	192.168.137.10	8.8.8.8	DNS	86	Standard query 0x6c49 PTR 145.219.34.89.in-addr.arpa
2015-08-20 15:58:45.568416000	92.86.33.125	192.168.137.10	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit
2015-08-20 15:58:45.844717000	192.168.137.10	8.8.8.8	DNS	86	Standard query 0x6c49 PTR 145.219.34.89.in-addr.arpa
2015-08-20 15:58:46.840639000	192.168.137.10	8.8.8.8	DNS	86	Standard query 0x6c49 PTR 145.219.34.89.in-addr.arpa
2015-08-20 15:58:47.001227000	8.8.8.8	192.168.137.10	DNS	86	Standard query response 0x6c49 Server failure
2015-08-20 15:58:47.003011000	192.168.137.10	89.34.219.145	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00>
2015-08-20 15:58:48.026383000	8.8.8.8	192.168.137.10	DNS	86	Standard query response 0x6c49 Server failure
2015-08-20 15:58:48.026451000	192.168.137.10	8.8.8.8	ICMP	114	Destination unreachable (Port unreachable)
2015-08-20 15:58:48.026628000	92.86.33.126	192.168.137.10	ICMP	120	Time-to-live exceeded (Time to live exceeded in transit
2015-08-20 15:58:48.494526000	192.168.137.10	89.34.219.145	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00>
2015-08-20 15:58:49.048622000	8.8.8.8	192.168.137.10	DNS	86	Standard query response 0x6c49 Server failure
2015-08-20 15:58:49.048685000	192.168.137.10	8.8.8.8	ICMP	114	Destination unreachable (Port unreachable)
2015-08-20 15:58:49.458021000	92.86.33.126	192.168.137.10	ICMP	120	Time-to-live exceeded (Time to live exceeded in transit
2015-08-20 15:58:49.993338000	192.168.137.10	89.34.219.145	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00>
2015-08-20 15:58:50.586707000	192.168.137.2	192.168.137.255	BROWSER	219	Become Backup Browser
2015-08-20 15:58:50.603117000	192.168.137.10	89.34.219.145	TCP	62	[TCP Retransmission] 49885→1604 [SYN] Seq=0 Win=8192 L

Process Monitor(Noriben)を使ってみました！



```
15:58:3...  dk5.exe  1668  RegSetInfoKey     HKLM¥SOFTWARE¥Policies¥Microsoft¥Windows¥System
15:58:3...  dk5.exe  1668  CreateFile        C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  SetEndOfFileInf...  C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  RegSetInfoKey     HKLM¥SOFTWARE¥Policies¥Microsoft¥Windows¥System
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
15:58:3...  dk5.exe  1668  WriteFile         C:¥Users¥test¥Documents¥MSDCSC¥msdcsc.exe
```

変なファイルが作成されている！！！

msdcsc.exe

16:45:4...	msdcsc.exe	896	RegSetInfoKey	HKCR¥Folder
16:45:4...	msdcsc.exe	896	RegSetInfoKey	HKCR¥AllFilesystemObjects
16:45:4...	msdcsc.exe	896	WriteFile	C:¥Users¥test¥AppData¥Roaming¥dclogs¥2015-08-20-5.dc
16:45:4...	msdcsc.exe	896	WriteFile	C:¥Users¥test¥AppData¥Roaming¥dclogs¥2015-08-20-5.dc
16:45:4...	msdcsc.exe	896	RegSetInfoKey	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run
16:45:4...	msdcsc.exe	896	RegSetValue	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run¥MicroUpd

2015-08-20-5.dc

キーロガー

```
:: Program Manager (16:37:06)


:: 89ef10cb2f88c5c56db1df063657249a.pcapng  [Wireshark 1.10.1  (SVN Rev 50926 from /trunk-1.10)] (16:37:26)
[DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN][DOWN]

:: 20150814_intern (¥¥vboxsrv) (E:) (16:38:04)


:: Program Manager (16:38:49)
b

:: Clipboard Change : size = 0 Bytes (16:38:49)


:: Program Manager (16:38:49)
dk5.exe
b

:: Clipboard Change : size = 0 Bytes (16:38:49)


:: 20150814_intern (¥¥vboxsrv) (E:) (16:41:40)

[<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-]


:: 20150814_intern (¥¥vboxsrv) (E:) (16:41:40)

[<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-][<-]
```

約1週間経ってもう一度このマルウェアを検証した結果

←アイコンが変わっていた！

12:23:40.3578751	Darkkomet.exe	4084	RegSetInfoKey	HKCU¥Software¥DC3_FEXEC
12:23:40.3579918	Darkkomet.exe	4084	RegSetInfoKey	HKCU¥Software¥DC3_FEXEC
12:23:40.3580900	Darkkomet.exe	4084	RegSetValue	HKCU¥Software¥DC3_FEXEC¥2015/08/27 at 12:23:40
12:23:40.3596614	Darkkomet.exe	4084	RegSetInfoKey	HKLM¥SOFTWARE¥Policies¥Microsoft¥Windows¥System
12:23:40.3606698	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥msdcsc.exe
12:23:40.3608137	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥msdcsc.exe
12:23:40.3609178	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥msdcsc.exe
12:23:40.3610063	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥msdcsc.exe
12:23:40.3610957	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥msdcsc.exe
12:23:40.3612182	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥msdcsc.exe
12:23:40.3625757	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥Bd9yxh8sdPcg¥msdcsc.exe
12:23:40.3626837	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥Bd9yxh8sdPcg¥msdcsc.exe
12:23:40.3628110	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥Bd9yxh8sdPcg¥msdcsc.exe
12:23:40.3629161	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥Bd9yxh8sdPcg¥msdcsc.exe
12:23:40.3630094	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥Bd9yxh8sdPcg¥msdcsc.exe
12:23:40.3630998	Darkkomet.exe	4084	CreateFile	C:¥Windows¥SysWOW64¥MSDCSC¥Bd9yxh8sdPcg¥msdcsc.exe
12:23:40.3634062	Darkkomet.exe	4084	RegSetInfoKey	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run
12:23:40.3635841	Darkkomet.exe	4084	RegSetValue	HKCU¥Software¥Microsoft¥Windows¥CurrentVersion¥Run¥MicroUpdate

←「mscdsc.exe」が作られている場所が違う

12:27:07.9627626	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT
12:27:07.9632216	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT
12:27:07.9636582	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT
12:27:07.9658306	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT
12:27:07.9676256	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT
12:27:07.9681896	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT
12:27:07.9687050	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT
12:27:07.9691941	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT
12:27:07.9696667	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT
12:27:07.9701023	msdcsc.exe	1276	WriteFile	C:¥Users¥nam¥NTUSER.DAT

←作られているものが違う

キーロガーファイルは
作られていないのか？

1週間前にキーロガーが作られているディレクトリを訪れてみた結果・・・

キーロガーは
作成されていた！

```
:: MSDCSC (11:43:17)



:: Clipboard Change : size = 139 Bytes (11:43:17)
C:¥Users¥nam¥AppData¥Local¥Microsoft¥Windows¥UsrClass.dat{c82c39b0-2bcf-11e3-a8d5-0800276d1ab2}.TMContainer00000000000000000002.regtrans-ms

:: 無題 - メモ帳 (11:43:50)
[<-]I enjoyed internship. Thank you for everything!!

:: 名前を付けて保存 (11:43:56)
ai


:: ai.txt - メモ帳 (11:44:25)
h

:: ドキュメント (11:44:40)
[<-]
```

Signature作成

- IPSに正規表現で書かれた文字列を登録しておくと、該当するマルウェアの実行を止める事ができる
- Signatureを作成するにあたって・・・
  - 検体のパターンを見つけることが重要
  - 沢山のマルウェアに触れることが大事
- 今回Signatureを作成する対象にしたのはCryptWall3.0
  - 分かりやすいパターンだったから
  - CryptWall3.0の検体を沢山触れたから

23d8f7a4b4668b64d5cc4c4a84edfe7d (CryptWall3.0)

Wiresharkで見た通信の1部

Source	Destination	Protocol	Length	Info
192.168.137.10	199.116.252.134	HTTP	708	GET /wp-content/themes/r.php?D0B1745184D4B19325F8CA239D78E8040A0972AFF24E5D0F8F9F536707F9FC68C46
199.116.252.134	192.168.137.10	TCP	60	80→49176 [RST] Seq=1 Win=2097152 Len=0
192.168.137.10	8.8.8.8	DNS	76	Standard query 0xe409 A shmetterheath.ru
8.8.8.8	192.168.137.10	DNS	92	Standard query response 0xe409 A 217.12.207.33
192.168.137.10	217.12.207.33	TCP	66	49177→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
217.12.207.33	192.168.137.10	TCP	66	80→49177 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK_PERM=1 WS=64
192.168.137.10	217.12.207.33	TCP	54	49177→80 [ACK] Seq=1 Ack=1 Win=65800 Len=0
192.168.137.10	217.12.207.33	HTTP	671	GET /wp-content/themes/r.php?D0B1745184D4B19325F8CA239D78E8040A0972AFF24E5D0F8F9F536707F9FC68C46
217.12.207.33	192.168.137.10	TCP	60	80→49177 [RST] Seq=1 Win=202144 Len=0
192.168.137.2	192.168.137.10	ICMP	82	Redirect (Redirect for network)
192.168.137.10	8.8.8.8	DNS	76	Standard query 0x6704 A fgainterests.com
8.8.8.8	192.168.137.10	DNS	92	Standard query response 0x6704 A 199.116.254.169
192.168.137.10	199.116.254.169	TCP	66	49178→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
199.116.254.169	192.168.137.10	TCP	60	80→49178 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400
192.168.137.10	199.116.254.169	TCP	54	49178→80 [ACK] Seq=1 Ack=1 Win=64400 Len=0
192.168.137.10	199.116.254.169	HTTP	671	GET /wp-content/themes/r.php?D0B1745184D4B19325F8CA239D78E8040A0972AFF24E5D0F8F9F536707F9FC68C46
199.116.254.169	192.168.137.10	TCP	60	80→49178 [RST] Seq=1 Win=4096 Len=0

今回CryptoWall3.0の検体、3種類から見つけ出せたパターン

r.php?D0B・・・から始まるパターン

・***GET /wp-content/themes/r.php?D0B1745184D4B19325F8CA239D78E8040A0972AFF24E5D0F8F9F536707F9FC68C46E87F65B51CDF4C5ACB0D6EB4DB2C038E57AD5276B81D65B1A0F9781F1BDD57FECBB1D7463979ECB13377C10FBD6382B595DBA6327EE73562219D2938743BE7CAACB09260AF6BC1B3048EC0E32F5D40151F3AC2B7F9BA0D5FC8E81F8CFBEA1F1AE9329F2D04271B80D71615974078FFC988A0DA2536E775E14E1A62E4AF79C***A1623287392AA0C8AFFDCE91D62C516011687CA5BE2EB4AA1E4038844B7003641539425646F1945FF2EAB0A7E5EC877AE736385D4DC9795F0C4472A81664C1FE

・***GET /wp-content/themes/r.php?D0B1745184D4B19325F8CA239D78E8040A0972AFF24E5D0F8F9F536707F9FC68C46E87F65B51CDF4C5ACB0D6EB4DB2C038E57AD5276B81D65B1A0F9781F1BDD57FECBB1D7463979ECB13377C10FBD6382B595DBA6327EE73562219D2938743BE7CAACB09260AF6BC1B3048EC0E32F5D40151F3AC2B7F9BA0D5FC8E81F8CFBEA1F1AE9329F2D04271B80D71615974078FFC988A0DA2536E775E14E1A62E4AF79C***3DF8CAC7E5307596E63D7F9164577C4F9A79A71BA4685FE3A26A42CF1E44C15EB4DE00EABE367D2F5CC169261338D6338FE8C589FA0757ACF19F49E9E9EE6E04

r.php?D3E・・・から始まるパターン

・***GET /wp-content/themes/r.php?D3ECA3EC23AA62A397F6CA71219BA2F0B3E6261788E14279B373E05E4CF372A61D876D79D6E9C1E7A6BFDFFEAE21ACB2BB9B34C663586CA52035797C21EBB034CA08AD02AFA2146A14F40AC50F55D23D1C9471FC874BCB9BEDABC741DD2DCBDB***5F2D63D51F813B2D9389429A07EFF94E18C2F4B1CBE39E029AFAB14E6A90E7766E981D2A26B41D0121B4805249B334F0D034E73AF1B2D484C2FCCAF587C913D1749DFC4880D87E09C6EF565926462E2B

・***GET /wp-content/themes/r.php?D3ECA3EC23AA62A397F6CA71219BA2F0B3E6261788E14279B373E05E4CF372A61D876D79D6E9C1E7A6BFDFFEAE21ACB2BB9B34C663586CA52035797C21EBB034CA08AD02AFA2146A14F40AC50F55D23D1C9471FC874BCB9BEDABC741DD2DCBDB***4CB46CCFD8E110FB5851003E91ABD49AC2522A7ADED9D54D9908A4E03BAFD721D830B34A15C9AECF0A02F8D5219DD19BC753E85BABD829F2A595027B30B1D48E3D0C55D58E45A6F083ABC69A999A3B93

実際に書いたSignatureとIPSの検知結果

Signature・・・「/[a-zA-Z]¥.php¥?[A-Z0-9]{300,}」

1000003	CryptoWall3_GET_NotVM		192.168.137.10	198.1.106.126	6 (TCP)	Global				26 Aug 2015 18:20:40
1000003	CryptoWall3_GET_NotVM		192.168.137.10	199.116.254.169	6 (TCP)	Global				26 Aug 2015 18:20:40
1000003	CryptoWall3_GET_NotVM		192.168.137.10	217.12.207.33	6 (TCP)	Global				26 Aug 2015 18:20:39
1000003	CryptoWall3_GET_NotVM		192.168.137.10	199.116.252.134	6 (TCP)	Global				26 Aug 2015 18:20:38
1000003	CryptoWall3_GET_NotVM		192.168.137.10	84.22.101.205	6 (TCP)	Global				26 Aug 2015 18:20:38
1000003	CryptoWall3_GET_NotVM		192.168.137.10	149.210.193.39	6 (TCP)	Global				26 Aug 2015 18:20:37
1000003	CryptoWall3_GET_NotVM		192.168.137.10	198.1.106.126	6 (TCP)	Global				26 Aug 2015 18:08:58
1000003	CryptoWall3_GET_NotVM		192.168.137.10	199.116.254.169	6 (TCP)	Global				26 Aug 2015 18:08:57
1000003	CryptoWall3_GET_NotVM		192.168.137.10	217.12.207.33	6 (TCP)	Global				26 Aug 2015 18:08:56
1000003	CryptoWall3_GET_NotVM		192.168.137.10	199.116.252.134	6 (TCP)	Global				26 Aug 2015 18:08:55
1000003	CryptoWall3_GET_NotVM		192.168.137.10	84.22.101.205	6 (TCP)	Global				26 Aug 2015 18:08:53
1000003	CryptoWall3_GET_NotVM		192.168.137.10	149.210.193.39	6 (TCP)	Global				26 Aug 2015 18:08:51
1000003	CryptoWall3_GET_NotVM		192.168.137.80	198.1.106.126	6 (TCP)	Global				26 Aug 2015 09:51:28
1000003	CryptoWall3_GET_NotVM		192.168.137.80	199.116.254.169	6 (TCP)	Global				26 Aug 2015 09:51:27
1000003	CryptoWall3_GET_NotVM		192.168.137.80	217.12.207.33	6 (TCP)	Global				26 Aug 2015 09:51:26
1000003	CryptoWall3_GET_NotVM		192.168.137.80	199.116.252.134	6 (TCP)	Global				26 Aug 2015 09:51:26
1000003	CryptoWall3_GET_NotVM		192.168.137.80	149.210.193.39	6 (TCP)	Global				26 Aug 2015 09:51:20

まとめ

- 同じファミリーであっても検体ごとに動作が異なる
- マルウェアは環境、時には時期にも依存している
- 1週間前と後で動作が変わるマルウェアも存在するため定期的にSignatureを書く必要がある
- 実機でやる場合はバックアップファイルを別の場所で保存する必要がある

マルウェア検証をしていて楽しかったこと、面白かったこと

- 検体によって、RSTが返ってきているのにしつこくRetransmissionで再送していたものもあれば諦めて違う通信を始めるものもあった
- 隠しファイルを作っていたこと
- Wiresharkで通信内容を見れて、Process Monitorで何をしているのかが分かったところ

インターンシップ終了後の課題

- 家でも同じような環境を構築してマルウェアの検証を続けていきたい
- 今回のインターンを通して得た知識を元に色々な人にマルウェアの奥深さと危険性を伝えたい

Special Thanks

- MSSの皆様
- 水谷さん、菊池さん
- 窪田さん

1ヶ月 間ありがとうございました！