MAN1: Tracking the Crypter and the Actor

In the world of malware crypters and packers are often time considered throwaway by researchers, it's also fairly common to use them as training tools for junior personnel. In a way most obfuscations are treated as training, learning or for games like CTF(Capture The Flag). So it's probably not surprising that lots of researchers don't pay much attention to these layers. These layers can be used especially when you find some of the more sophisticated ones that tend to stick around for longer periods of time. While probably not as useful as tracking an actor to a backend system, these malware artifacts can provide valuable clues, serving as tools, techniques and procedures (TTPs) in tracking the ongoing operations of a specific threat actor across a wide range of operations and groups. In this case, we focus on MAN1, a sophisticated crypter dating back to 2014 that's still in use today.

The Actor

Associating an actor to a string of campaigns is never an easy task. Crimeware operates like an underground business -- multiple players may be involved in one project, pieces of an operation may be outsourced at any time, and elements can be handled by multiple groups over time. In these instances, it becomes harder to prove that the same criminal group is behind a string of malware campaigns stretching back two years.

However, subtle tricks and routines found in packers and crypters provide valuable clues for threat researchers. In some cases, it's possible to associate actors with their payloads, which allows threat researchers to track the movement of specific actors over time. Given the utility of these obfuscation techniques, actors often keep their tricks of the trade private and do not sell them to the masses on the underground.

One actor, or group, using such tricks is MAN1. We've associated MAN1 with Dyre, a trojan first used in large-scale campaigns targeting customers of major financial institutions and later used to target organizations in additional sectors that include technology, petrochemical and others. The MAN1 moniker comes from the binaries the Dyre malware downloads from compromised websites. These downloaded files usually included a man1.exe file, which was typically an older version of Dyre.

Tracking MAN1

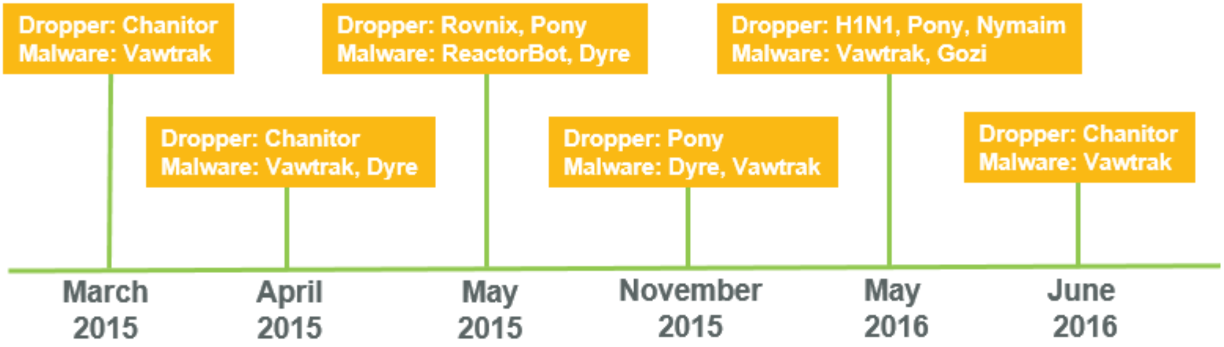
To link MAN1 to Dyre, we had to take a look at earlier campaigns. Before Dyre, these actors used Chanitor to download Vawtrak, a banking trojan. The server delivering Chanitor used "bulletproof hosting", which are hosting services permitting extreme leniency in their terms of service. Later, this actor gradually began delivering both Vawtrak and Dyre. Eventually, the actor began delivering Dyre exclusively. The servers used at the beginning of this transition hold an important clue to uncover the identity of the actor: These same few servers were also used to deliver Vawtrak using Chanitor.

As with most long-established actors, MAN1 exhibits distinct TTPs in performing their ongoing malicious activities. The crypter discussed here is one such tool used by this actor since its involvement in Vawtrak in 2014, and possibly earlier. While crypters are relatively common, really good crypters -- designed to prevent detection through various methods -- can sell for a lot of money on the underground, where they typically remain private and used for a very long time.

The uniqueness and complexity of the crypter, coupled with the other TTPs used by this group, provides another valuable clue and paints a clearer picture of the actor. Over time, the research community picked up on this actor's subtleties, such as its consistent use of ‘feedweb_data’ or ‘cached_data’ folders on compromised websites. These characteristics made it possible for researchers to track this actor's involvement across multiple malware families over two years’ time.

A Timeline of Exploits

Let's take a look at MAN1's activities beginning in March 2015.



March 2015: Chanitor, Vawtrak: By tracing the IP range by naming schemes and crypter usage, we find the actor's first involvement with Vawtrak, when it spammed out Chanitor as a flight confirmation (1) to deliver Vawtrak from 91.194.254.213/us/file.jpg.

April 2015: Chanitor -> Vawtrak, Dyre: In April 2015, we spotted a glaring association with this actor's involvement in both Dyre and the old Vawtrak in a spam campaign (2) that used a macro to download a text file that contained the url to the payload. This technique provides the actor flexibility, in that they can use the same spam campaign to deliver multiple payloads. This technique has one drawback: It needs to burn through extra compromised websites. This campaign had two payloads – one from 91.194.254.235/uss/file.exe using Chanitor (delivering Vawtrak) and one from 91.194.254.222/us2/file.exe delivering Dyre. The Dyre sample used in this campaign was named ‘man1’. This IP range used can be traced back further -- to Chanitor delivering old Vawtrak -- and was also used for testing the newer Vawtrak seen today.

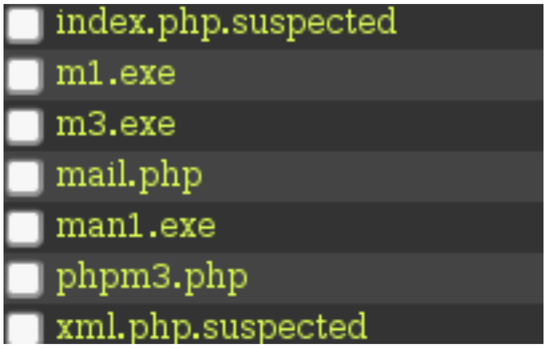
May 2015: Rovnix, Pony -> ReactorBot: This actor has shown interest in using the newest malware within the crimeware domain. In May 2015, a new banker emerged and was distributed using Rovnix as a dropper. The downloaded and loaded DLL was named ReactorDemo.dll, and was named ReactorBot (3). This actor was involved in a spam run delivering CVE-2014-1761 that exploited RTFs delivering Pony, which would then download ReactorBot from locations such as:

Encentivhealth[.]m/wp-content/plugins/cached_data/n1.exe

Also in May, we see this actor using a similar naming structure on compromised websites to deliver Dyre, which was identified as a MAN1 campaign within the research community, from macro docs downloading Pony. In this instance, we see one of the compromised website folder structures exhibit characteristics used by this actor:

Cyctechnology[.]com/wp-content/plugins/cached_data/m1.exe

The /cached_data/ structure is probably familiar to some from frequent Dyre spamming. Why use the same naming structure on compromised websites? Our guess is that it's an automated process as demonstrated when you examine the contents of that folder across multiple servers.



□ index.php.suspected
□ m1.exe
□ m3.exe
□ mail.php
□ man1.exe
□ phpm3.php
□ xml.php.suspected

November 2015: Dyre, Vawtrak: In early November 2015, we witnessed one of the Dyre actors transition from Dyre to the updated version of Vawtrak. This actor continued to deliver both Dyre and Vawtrak during multiple spam campaigns on November 2, 2015 (5, 6). The timing of this transition raises suspicions, as it corresponded with a Dyre takedown event later that same month (4). For the Dyre run, we see the /sliva/ structure for the Pony runs (cd445e52eb7d2ca7359a8513157dd0a9), which is still used today for campaigns delivering Vawtrak.

May 2016: H1N1 -> Pony, Vawtrak, Nymaim -> Gozi: Earlier, on May 25, 2016, researchers observed a spam campaign delivering Vawtrak and using similar techniques. But instead of Chanitor, the loader was H1N1 downloading Pony as pm.dll and Vawtrak as inst.exe.

Also of note is this actor's recent use of Nymaim from spammed out macro documents dropping Pony (7). These documents would download Nymaim from places such as:

elfielatorestaurante[.]com/wp-content/plugins/cached_data/print[.]exe

It would then deliver a Gozi/ISFB module targeting US entities*. This delivery was later coined GozNym due to the custom work linking the Gozi/ISFB module to Nymaim (8).

* A portion of these targets can be found toward the end of this post.

June 2016: H1N1, Chanitor/Hancitor -> Vawtrak: Recently, this actor pushed Vawtrak heavily using a variety of delivery methods. Two methods seen recently are H1N1 and a Chanitor variant (also called Hancitor). These campaigns are noteworthy for the aforementioned crypter and the tactics it uses. One such tactic involves delivering Pony separately from Vawtrak, even though Vawtrak comes with a stealer module component. This actor has also been observed using the same Pony gate structure of '/sl/gate.php' or '/zapoy/gate.php'. A recent campaign on June 7, 2016 utilized a Word document dropper using names that followed a pattern of 'report_\d{7}.doc' to deliver a Chanitor variant that would check-in to a gate with the uri '/sl/gate.php' and then download both Pony and Vawtrak.

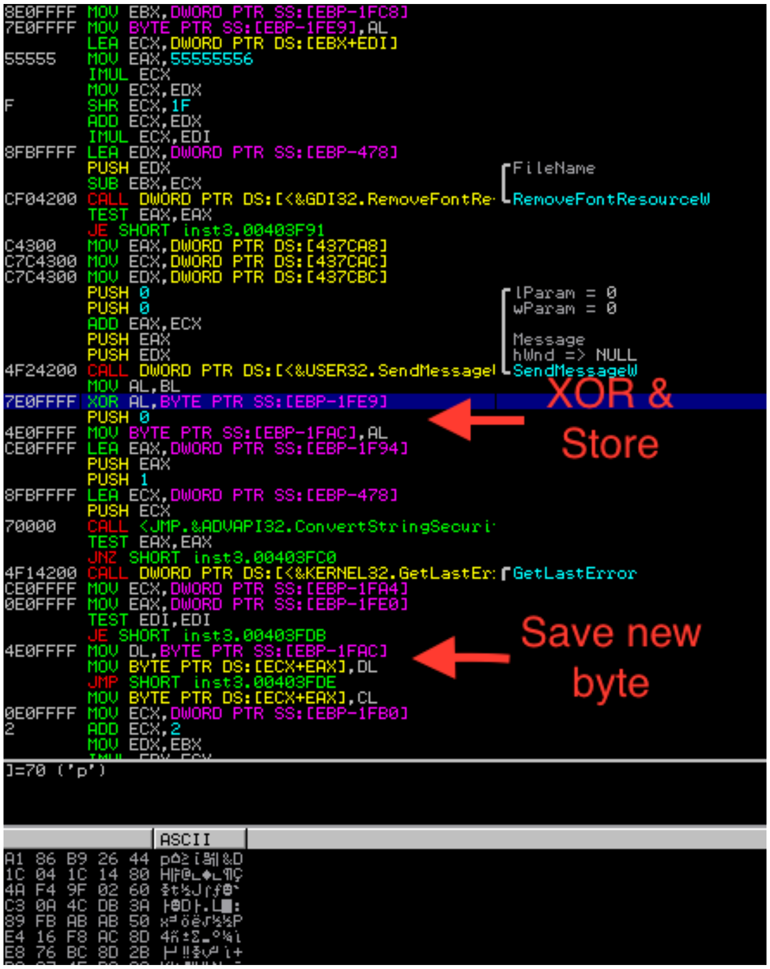
Also of note on these recent campaigns is the man1.exe file that may show up on compromised websites. This can be seen on a campaign from June 20, 2016, in which H1N1 delivered the usual Pony and Vawtrak malware. However, if we look a little closer at the website, it downloads Pony from ('crr-medvezonok[.]ru/about/pm.dll') and we find a number of other executables residing on that server in that same subfolder ('inst1.exe', 'inst2.exe', 'inst3.exe', 'man1.exe'). The executable man1.exe is actually an old unpacked Dyre malware sample -- further pointing to this actor's previous involvement in Dyre.

Latest: To date, the actor continues using the MAN1 crypter. The actor sticks to the same naming scheme for up to months at a time. These consistent TTPs could be due to a number of reasons: The actor may be using a toolkit or buying mass quantities of shelled servers from the same entity and going through them systematically. Either way, by identifying these key characteristics, we narrowed in on an actor's use of this custom crypter, which then made it possible for us to trace this actor's movement across multiple malware families over years. We've found other notable malware associated with this actor by following the crypter's evolution over time. This malware includes a P2P Gozi variant, CTB Locker and Andromeda.

Peeling Back the Layers of the Crypter

A crypter, in its basic form, is designed to obfuscate code. Researchers commonly have to break through layers of crypters or packers in order to get to the underlying malware code, it becomes instinctive for anyone who researchers malware for very long. Some crypters used for malware add functions, such as anti-virtualization or anti-sandboxing. The problem with most crypters is that they are a fire-and-forget tool used to bypass antivirus and sandbox detections. Some crypters employ a more drastic technique in which they use multiple layers that involve dynamically generated code. MAN1 is one such advanced crypter.

While it is often tempting to break through all the layers to get to the heart of the malware, our research supports the idea that sometimes these discarded layers can be used to bridge the gap and turn research into intelligence to help profile actors. The first layer is mostly just a bunch of deadcode with limited functionality, but it allows quite a bit of throwaway code to be added. This deadcode can be added for numerous reasons -- from throwing off sandbox reports, to messing with AV heuristics and generally making it a pain to signature off of. Eventually the code will decode the next layer, which is where most of the real work can begin. Usually, this first layer will be XOR decoded, but will be surrounded by a large amount of useless code operating on Windows or fonts that don't exist.



```
8E0FFFF MOV EBX,DWORD PTR SS:[EBP-1FC8]
7E0FFFF MOV BYTE PTR SS:[EBP-1FE9],AL
        LEA ECX,DWORD PTR DS:[EBX+EDI]
55555   MOV EAX,55555556
        IMUL ECX
        MOV ECX,EDX
F       SHR ECX,1F
        ADD ECX,EDX
        IMUL ECX,EDI
8FBFFFF LEA EDX,DWORD PTR SS:[EBP-478]
        PUSH EDX                                 ┌FileName
        SUB EBX,ECX                              │
CF04200 CALL DWORD PTR DS:[<&GDI32.RemoveFontRe· └RemoveFontResourceW
        TEST EAX,EAX
        JE SHORT inst3.00403F91
C4300   MOV EAX,DWORD PTR DS:[437CA8]
C7C4300 MOV ECX,DWORD PTR DS:[437CAC]
C7C4300 MOV EDX,DWORD PTR DS:[437CBC]
        PUSH 0                                   ┌lParam = 0
        PUSH 0                                   │wParam = 0
        ADD EAX,ECX                              │
        PUSH EAX                                 │Message
        PUSH EDX                                 │hWnd => NULL
4F24200 CALL DWORD PTR DS:[<&USER32.SendMessageW └SendMessageW
        MOV AL,BL
7E0FFFF XOR AL,BYTE PTR SS:[EBP-1FE9]
        PUSH 0
4E0FFFF MOV BYTE PTR SS:[EBP-1FAC],AL
CE0FFFF LEA EAX,DWORD PTR SS:[EBP-1F94]
        PUSH EAX
        PUSH 1
8FBFFFF LEA ECX,DWORD PTR SS:[EBP-478]
        PUSH ECX
70000   CALL <JMP.&ADVAPI32.ConvertStringSecuri·
        TEST EAX,EAX
        JNZ SHORT inst3.00403FC0
4F14200 CALL DWORD PTR DS:[<&KERNEL32.GetLastEr: ┌GetLastError
CE0FFFF MOV ECX,DWORD PTR SS:[EBP-1FA4]
0E0FFFF MOV EAX,DWORD PTR SS:[EBP-1FE0]
        TEST EDI,EDI
        JE SHORT inst3.00403FDB
4E0FFFF MOV DL,BYTE PTR SS:[EBP-1FAC]
        MOV BYTE PTR DS:[ECX+EAX],DL
        JMP SHORT inst3.00403FDE
        MOV BYTE PTR DS:[ECX+EAX],CL
0E0FFFF MOV ECX,DWORD PTR SS:[EBP-1FB0]
2       ADD ECX,2
        MOV EDX,EBX
]=70 ('p')
```

```
A1 86 B9 26 44 p⌂≥ï╣&D
1C 04 1C 14 80 H╟@∟♦∟¶Ç
4A F4 9F 02 60 ╪t½J⌠ƒ☻`
C3 0A 4C DB 3A ├◙D├.L█:
89 FB AB AB 50 ë√öë√½½P
E4 16 F8 AC 8D 4ñ±Σ▬°¼ì
E8 76 BC 8D 2B ┣‼╪v╝ì+
```

The second and third layers function roughly the same as the first, with the exception of decoding. The second layer decodes the output of the first layer and the third layer decodes the output of the second.

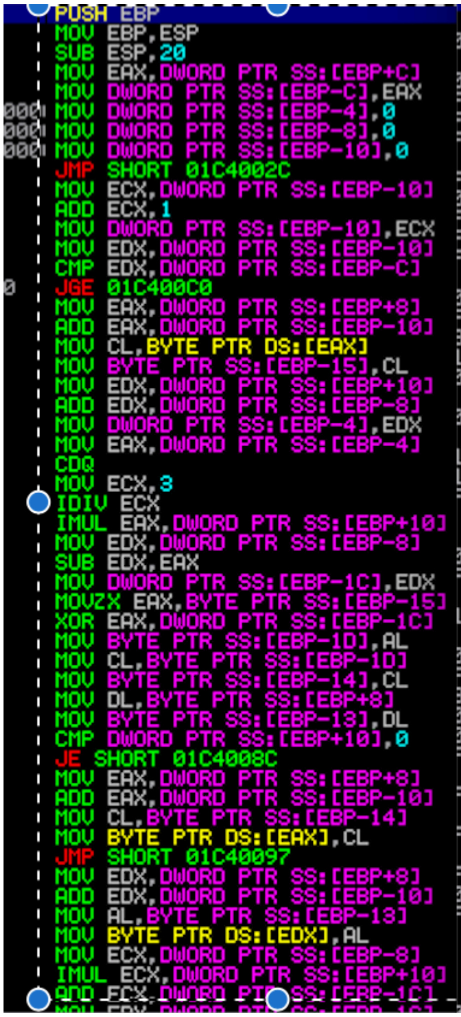
Each layer shares the following common characteristics:

- Is numbered
- Contains variable length, numbered chunks
- Each chunk may be compressed

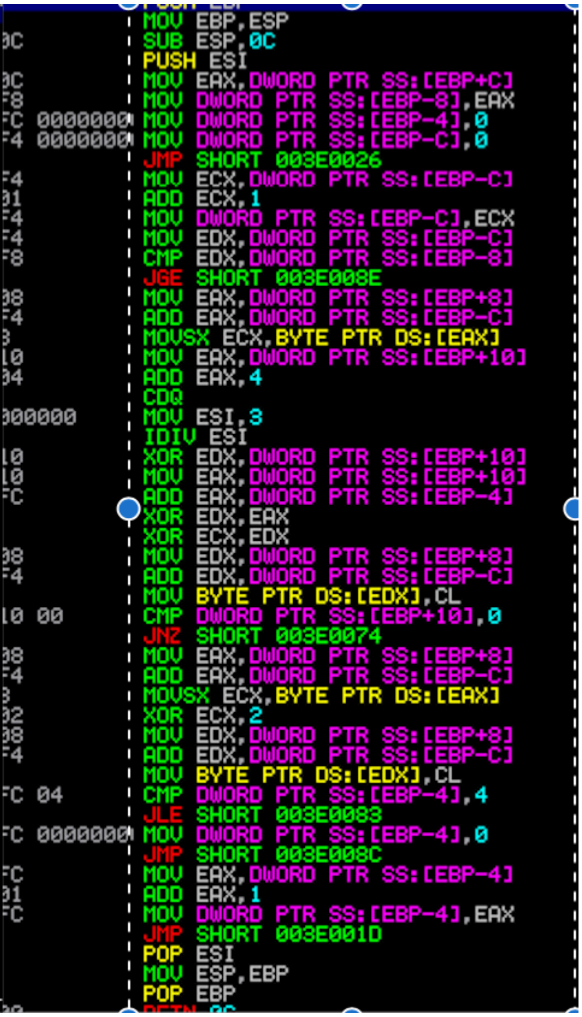
To accommodate this setup, each chunk has an attached header as shown in this mock up:

```
struct DataBlob {
  unsigned short CheckVal1;
  unsigned short CheckVal2;
  unsigned short CheckOffset;
  struct ChunkHeader {
    unsigned int SetNum;
    unsigned int length;
    unsigned int SetIndex;
    unsigned int check;
    unsigned int key;
    unsigned int compressedflag;
    unsigned int uncompressedSize;
  }chunk;
  char data[chunk.length];
}
```

As the layer performs its decoding routine, it utilizes shellcode that is decoded and reassembled for every chunk in the next layer. This shellcode is then used to decode the data in the found chunk. The same shellcode is used on all layers, but differs from sample to sample. This characteristic leads us to believe it is dynamically generated to perform various types of decoding operations and keys on the layers. By comparing this layer between two different samples delivered on the same day, we can see slight differences. This means the layer is generated when the crypt happens on the payload because it is required to encode the payload.

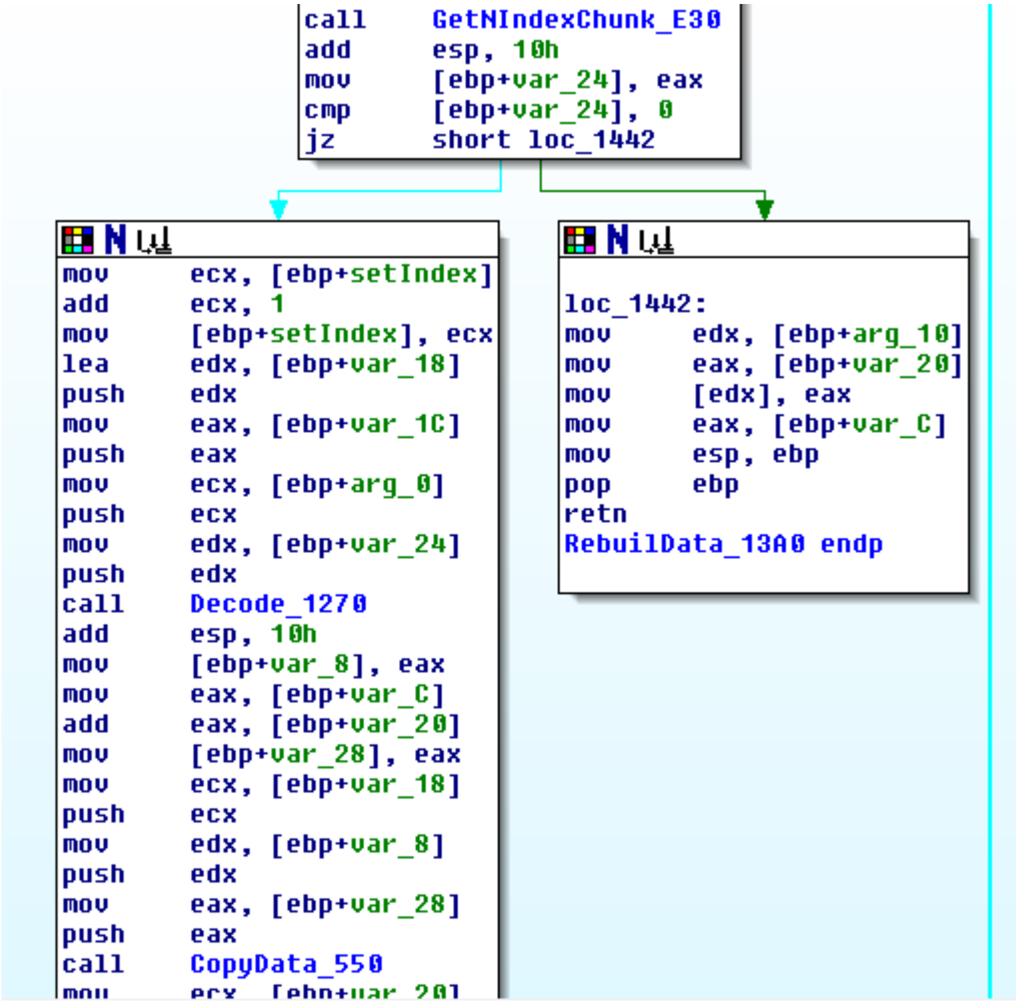


```
PUSH EBP
MOV EBP,ESP
SUB ESP,20
MOV EAX,DWORD PTR SS:[EBP+C]
MOV DWORD PTR SS:[EBP-C],EAX
MOV DWORD PTR SS:[EBP-4],0
MOV DWORD PTR SS:[EBP-8],0
MOV DWORD PTR SS:[EBP-10],0
JMP SHORT 01C4002C
MOV ECX,DWORD PTR SS:[EBP-10]
ADD ECX,1
MOV DWORD PTR SS:[EBP-10],ECX
MOV EDX,DWORD PTR SS:[EBP-10]
CMP EDX,DWORD PTR SS:[EBP-C]
JGE 01C400C0
MOV EAX,DWORD PTR SS:[EBP+8]
ADD EAX,DWORD PTR SS:[EBP-10]
MOV CL,BYTE PTR DS:[EAX]
MOV BYTE PTR SS:[EBP-15],CL
MOV EDX,DWORD PTR SS:[EBP+10]
ADD EDX,DWORD PTR SS:[EBP-8]
MOV DWORD PTR SS:[EBP-4],EDX
MOV EAX,DWORD PTR SS:[EBP-4]
CDQ
MOV ECX,3
IDIV ECX
IMUL EAX,DWORD PTR SS:[EBP+10]
MOV EDX,DWORD PTR SS:[EBP-8]
SUB EDX,EAX
MOV DWORD PTR SS:[EBP-1C],EDX
MOVZX EAX,BYTE PTR SS:[EBP-15]
XOR EAX,DWORD PTR SS:[EBP-1C]
MOV BYTE PTR SS:[EBP-1D],AL
MOV CL,BYTE PTR SS:[EBP-1D]
MOV BYTE PTR SS:[EBP-14],CL
MOV DL,BYTE PTR SS:[EBP+8]
MOV BYTE PTR SS:[EBP-13],DL
CMP DWORD PTR SS:[EBP+10],0
JE SHORT 01C4008C
MOV EAX,DWORD PTR SS:[EBP+8]
ADD EAX,DWORD PTR SS:[EBP-10]
MOV CL,BYTE PTR SS:[EBP-14]
MOV BYTE PTR DS:[EAX],CL
JMP SHORT 01C40097
MOV EDX,DWORD PTR SS:[EBP+8]
ADD EDX,DWORD PTR SS:[EBP-10]
MOV AL,BYTE PTR SS:[EBP-13]
MOV BYTE PTR DS:[EDX],AL
MOV ECX,DWORD PTR SS:[EBP-8]
IMUL ECX,DWORD PTR SS:[EBP+10]
ADD ECX,DWORD PTR SS:[EBP-1C]
```



```
MOV EBP,ESP
SUB ESP,0C
PUSH ESI
MOV EAX,DWORD PTR SS:[EBP+C]
MOV DWORD PTR SS:[EBP-8],EAX
MOV DWORD PTR SS:[EBP-4],0
MOV DWORD PTR SS:[EBP-C],0
JMP SHORT 003E0026
MOV ECX,DWORD PTR SS:[EBP-C]
ADD ECX,1
MOV DWORD PTR SS:[EBP-C],ECX
MOV EDX,DWORD PTR SS:[EBP-C]
CMP EDX,DWORD PTR SS:[EBP-8]
JGE SHORT 003E008E
MOV EAX,DWORD PTR SS:[EBP+8]
ADD EAX,DWORD PTR SS:[EBP-C]
MOVSX ECX,BYTE PTR DS:[EAX]
MOV EAX,DWORD PTR SS:[EBP+10]
ADD EAX,4
CDQ
MOV ESI,3
IDIV ESI
XOR EDX,DWORD PTR SS:[EBP+10]
MOV EAX,DWORD PTR SS:[EBP+10]
ADD EAX,DWORD PTR SS:[EBP-4]
XOR EDX,EAX
XOR ECX,EDX
MOV EDX,DWORD PTR SS:[EBP+8]
ADD EDX,DWORD PTR SS:[EBP-C]
MOV BYTE PTR DS:[EDX],CL
CMP DWORD PTR SS:[EBP+10],0
JNZ SHORT 003E0074
MOV EAX,DWORD PTR SS:[EBP+8]
ADD EAX,DWORD PTR SS:[EBP-C]
MOVSX ECX,BYTE PTR DS:[EAX]
XOR ECX,2
MOV EDX,DWORD PTR SS:[EBP+8]
ADD EDX,DWORD PTR SS:[EBP-C]
MOV BYTE PTR DS:[EDX],CL
CMP DWORD PTR SS:[EBP-4],4
JLE SHORT 003E0083
MOV DWORD PTR SS:[EBP-4],0
JMP SHORT 003E008C
MOV EAX,DWORD PTR SS:[EBP-4]
ADD EAX,1
MOV DWORD PTR SS:[EBP-4],EAX
JMP SHORT 003E001D
POP ESI
MOV ESP,EBP
POP EBP
```

Here we can see the main loop from one sample employing this technique:



```
call    GetNIndexChunk_E30
add     esp, 10h
mov     [ebp+var_24], eax
cmp     [ebp+var_24], 0
jz      short loc_1442
```

```
mov     ecx, [ebp+setIndex]
add     ecx, 1
mov     [ebp+setIndex], ecx
lea     edx, [ebp+var_18]
push    edx
mov     eax, [ebp+var_1C]
push    eax
mov     ecx, [ebp+arg_0]
push    ecx
mov     edx, [ebp+var_24]
push    edx
call    Decode_1270
add     esp, 10h
mov     [ebp+var_8], eax
mov     eax, [ebp+var_C]
add     eax, [ebp+var_20]
mov     [ebp+var_28], eax
mov     ecx, [ebp+var_18]
push    ecx
mov     edx, [ebp+var_8]
push    edx
mov     eax, [ebp+var_28]
push    eax
call    CopyData_550
mov     ecx, [ebp+var_20]
```

```
loc_1442:
mov     edx, [ebp+arg_10]
mov     eax, [ebp+var_20]
mov     [edx], eax
mov     eax, [ebp+var_C]
mov     esp, ebp
pop     ebp
retn
RebuilData_13A0 endp
```

Getting through the crypter is trivial. Breaking on kernel32!VirtualAlloc results in returning to the main loop of the layer as each calls VirtualAlloc every time it goes to reconstruct the shellcode layer. Adding a breakpoint to the end of that loop (the instruction just after kernel32!VirtualAlloc) presents the next layer. From there, execute 'till return' twice and then the next call will copy over the reconstructed code segment and a JMP.

Conclusion

Intimate knowledge of the crypter and other techniques have allowed us to tie numerous campaigns over the years to a single actor or group. We're aware that other researchers have identified some of these threads and our intention behind publishing this body of knowledge is to encourage others to recognize MAN1 and help build a fuller profile. The criminal landscape is vast, but there are often significant volumes of activity spanning campaigns and malware families that tie back to individual actors or groups.

References

1: https://techhelplist.com/spam-list/742-order-confirmation-for-flight-malware

2: https://techhelplist.com/spam-list/785-payment-confirmation-for-tax-refund-request-malware

3: http://www.kernelmode.info/forum/viewtopic.php?f=16&t=981&start=70#p25915

4: http://www.scmagazine.com/dyre-trojan-almost-dead-after-takedown-by-the-russians/article/472074/

5: https://techhelplist.com/spam-list/957-e-ticket-confirmation-aa-malware

6: https://myonlinesecurity.co.uk/american-airlines-e-ticket-confirmation-word-doc-malware/

7: https://techhelplist.com/spam-list/995-re-recipient-domain-name-sucks-malware

8: https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/

IOCs:

Chanitor:

o3qz25zwu4or5mak[.]tor2web[.]org/gate.php
xdndo2okt43cjx44[.]tor2web.blutmagie[.]de/gate.php
xdndo2okt43cjx44[.]tor2web[.]fi/gate.php
xdndo2okt43cjx44[.]tor2web[.]org/gate.php
um6fsdil5ecma5kf[.]tor2web.blutmagie[.]de/gate.php
mps23[.]ru/libraries/fof/controller/1304.exe
buloftoty[.]com/sl/gate.php
buloftoty[.]com/sl/gate.php
letatandone[.]ru/sl/gate.php
nkdoscqnp3myjiyr.onion[.]to/sl/gate.php
buzines24[.]ru/source/pm.dll
buzines24[.]ru/source/inst1.exe

95914f3cb47e2d200408456abc2fc277
63cc107d6f4464eb311324f950386b9f
db36c2f4db086a7f8e483187289e1c93
f5efd86c80538e104503c309e458efa9

Vawtrak:

hartwelstay[.]com/stats/00/counter/0000003A/56EB9C2B
weltfarystar[.]com/stats/00/counter/0000003A/56EB9C2B
rewdepehat[.]ru/stats/00/counter/0000003A/56EB9C2B

```
uldryledda[.]ru/stats/00/counter/0000003A/56EB9C2B
uldfiparevent[.]ru/stats/00/counter/0000003A/56EB9C2B
roldinglygo[.]ru/stats/00/counter/0000003A/56EB9C2B
perundmaheg[.]ru/stats/00/counter/0000003A/56EB9C2B
velyama[.]com/stats/00/counter/0000003A/56EB9C2B
shumines[.]com/stats/00/counter/0000003A/56EB9C2B
ceglolu[.]com/stats/00/counter/0000003A/56EB9C2B
ceglolu[.]com/stats/02/counter/0000003A/56EB9C2B
dunella[.]net/upd/58?id=1458281515&o=4&n=5
greatcountrygor[.]ru/stats/00/counter/0000006E/56EB9C2B
firstforestmonth[.]ru/stats/00/counter/0000006E/56EB9C2B
hornetwart[.]ru/stats/00/counter/0000006E/56EB9C2B
weronpalace[.]ru/stats/00/counter/0000006E/56EB9C2B
westnerthgom[.]ru/stats/00/counter/0000006E/56EB9C2B
dorthgornet[.]com/stats/00/counter/0000006E/56EB9C2B
andheduse[.]ru/stats/00/counter/0000006E/56EB9C2B
rinheca[.]ru/stats/00/counter/0000006E/56EB9C2B
etningand[.]ru/stats/00/counter/0000006E/56EB9C2B
termyen[.]ru/stats/00/counter/0000006E/56EB9C2B
haptalher[.]ru/stats/00/counter/0000006E/56EB9C2B
robonwas[.]ru/stats/00/counter/0000006E/56EB9C2B
wassinrat[.]ru/stats/00/counter/0000006E/56EB9C2B
parowheck[.]ru/stats/00/counter/0000006E/56EB9C2B
pergeca[.]ru/stats/00/counter/0000006E/56EB9C2B
astramanton[.]com/stats/00/counter/0000006E/56EB9C2B
haptedidti[.]ru/stats/00/counter/0000006E/56EB9C2B
betpeharrep[.]ru/stats/00/counter/0000006E/56EB9C2B
tothetinbu[.]ru/stats/00/counter/0000006E/56EB9C2B
wawronbonot[.]ru/stats/00/counter/0000006E/56EB9C2B
freeseathere[.]com/stats/00/counter/0000006E/56EB9C2B
gerbertdowen[.]com/stats/00/counter/0000006E/56EB9C2B
hertgotlitt[.]ru/stats/00/counter/0000006E/56EB9C2B
weasterd[.]com/stats/00/counter/0000006E/56EB9C2B
ronughmeligh[.]ru/stats/00/counter/0000006E/56EB9C2B
parwoonetons[.]ru/stats/00/counter/0000006E/56EB9C2B
sahissofreb[.]ru/stats/00/counter/0000006E/56EB9C2B
etdidnrowrab[.]ru/stats/00/counter/0000006E/56EB9C2B
sedsparkeun[.]ru/stats/00/counter/0000006E/56EB9C2B
righhowhanin[.]ru/stats/00/counter/0000006E/56EB9C2B
ketretdidnbe[.]ru/stats/00/counter/0000006E/56EB9C2B
kedathenrit[.]ru/stats/00/counter/0000006E/56EB9C2B
fonotoftret[.]ru/stats/00/counter/0000006E/56EB9C2B
drawnearme[.]ru/stats/00/counter/0000006E/56EB9C2B
fivelisterman[.]ru/stats/00/counter/0000006E/56EB9C2B
newquietlist[.]ru/stats/00/counter/0000006E/56EB9C2B
weoplitu[.]ru/stats/00/counter/0000006E/56EB9C2B
sdertunclis[.]ru/stats/00/counter/0000006E/56EB9C2B
betadvalyf[.]ru/stats/00/counter/0000006E/56EB9C2B
```

pwinmoxyfe[.]ru/stats/00/counter/0000006E/56EB9C2B
lazmestah[.]ru/stats/00/counter/0000006E/56EB9C2B
fortwronsit[.]ru/stats/00/counter/0000006E/56EB9C2B
lestrinate[.]com/stats/00/counter/0000006E/56EB9C2B
withreshersgot[.]ru%2520/stats/00/counter/0000006E/56EB9C2B
natosinhem[.]ru/stats/00/counter/0000006E/56EB9C2B
winfertrow[.]com/stats/00/counter/0000006E/56EB9C2B
quirtenatel[.]com/stats/00/counter/0000006E/56EB9C2B
masterstargon[.]ru/stats/00/counter/0000006E/56EB9C2B
laskrowler[.]ru/stats/00/counter/0000006E/56EB9C2B
uznatus[.]com/stats/00/counter/0000006E/56EB9C2B
cakedhisjohn[.]com/stats/00/counter/0000006E/56EB9C2B
idthentehed[.]com/stats/00/counter/0000006E/56EB9C2B
rebteugrigh[.]com/stats/00/counter/0000006E/56EB9C2B
othersforrep[.]com/stats/00/counter/0000006E/56EB9C2B
shumines[.]com/stats/00/counter/0000006E/56EB9C2B
perundmaheg[.]ru/stats/00/counter/0000006E/56EB9C2B
penothec[.]ru/stats/00/counter/0000006E/56EB9C2B
dowronrab[.]ru/stats/00/counter/0000006E/56EB9C2B
melebet[.]ru/stats/00/counter/0000006E/56EB9C2B
fawilut[.]ru/stats/00/counter/0000006E/56EB9C2B
dorthgornet[.]com/stats/00/counter/0000006E/56EB9C2B
fastrevertnom[.]com/stats/00/counter/0000006E/56EB9C2B
wergilesrest[.]com/stats/00/counter/0000006E/56EB9C2B
polnerfirst[.]com/stats/00/counter/0000006E/56EB9C2B
azmyto[.]ru/stats/00/counter/0000006E/56EB9C2B
mgsmedia[.]ru/Work/new/index.php
textidea[.]com/Work/new/index.php
vintageselects[.]com/Work/new/index.php
pausephone[.]com/Work/new/index.php
hybridtrend[.]com/Work/new/index.php
basislabel[.]com/Work/new/index.php
finehotels[.]net/Work/new/index.php
circlewear[.]net/Work/new/index.php
helloalliance[.]net/Work/new/index.php
seaboy[.]net/Work/new/index.php
wildclick[.]net/Work/new/index.php
camelcap[.]com/Work/new/index.php
ideagreens[.]com/Work/new/index.php
guesstrade[.]com/Work/new/index.php
castuning[.]ru/Work/new/index.php
basislabel[.]com/Work/new/index.php
camelcap[.]com/Work/new/index.php
castuning[.]ru/Work/new/index.php
circlewear[.]net/Work/new/index.php
finehotels[.]net/Work/new/index.php
guesstrade[.]com/Work/new/index.php
helloalliance[.]net/Work/new/index.php

hybridtrend[.]com/Work/new/index.php
ideagreens[.]com/Work/new/index.php
mgsmedia[.]ru/Work/new/index.php
ninthclub[.]com/Work/new/index.php
seaboy[.]net/Work/new/index.php
basislabel[.]com/Work/new/index.php
camelcap[.]com/Work/new/index.php
castuning[.]ru/Work/new/index.php
circlewear[.]net/Work/new/index.php
finehotels[.]net/Work/new/index.php
guesstrade[.]com/Work/new/index.php
helloalliance[.]net/Work/new/index.php
hybridtrend[.]com/Work/new/index.php
ideagreens[.]com/Work/new/index.php
mgsmedia[.]ru/Work/new/index.php
ninthclub[.]com/Work/new/index.php
pausephone[.]com/Work/new/index.php
seaboy[.]net/Work/new/index.php
textidea[.]com/Work/new/index.php
vintageselects[.]com/Work/new/index.php
wildclick[.]net/Work/new/index.php
foundingcast[.]com/rss/feed/stream
dringeraout[.]com/rss/feed/stream
broilerona[.]com/rss/feed/stream
bookeranto[.]com/rss/feed/stream
vineriadana[.]com/rss/feed/stream
greyscrolling[.]com/rss/feed/stream
solidarepapero[.]com/rss/feed/stream
svenorta[.]com/rss/feed/stream
goodtrade[.]bid/rss/feed/stream
todaywith[.]date/rss/feed/stream
quicklinks[.]download/rss/feed/stream
beproudof[.]faith/rss/feed/stream
takeaphoto[.]loan/rss/feed/stream
oldblackman[.]party/rss/feed/stream
fastblackspeed[.]racing/rss/feed/stream
cangetyour[.]review/rss/feed/stream
epicsimple[.]science/rss/feed/stream
fastandeasy[.]trade/rss/feed/stream
seeyounow[.]webcam/rss/feed/stream
championinred[.]win/rss/feed/stream
chalengeforyou[.]win/rss/feed/stream
cookingwithme[.]date/rss/feed/stream
vigriada[.]com/rss/feed/stream
fugredoma[.]com/rss/feed/stream
edreciano[.]com/rss/feed/stream
derfeicon[.]com/rss/feed/stream
boelongo[.]com/rss/feed/stream

baberigia[.]com/rss/feed/stream
pachuliko[.]com/rss/feed/stream
tuberosan[.]com/rss/feed/stream

e3b6acf4ccd7f0257d201977bb600e04
feb49bde382fec4c821e4e608d0134f5
6d046ea72343a1e49c8f3932ea7f6c75
7fc75215d5502cdd1ff5413d2a882331
77561141a0f15ff56c70995c4f1ddc98
5238cd34caae600b3f592e2595aa6949
6fad86a0fcc912f32474f6c7a86fe37a
fb4d250b6a733ce4f5c583e9ebb667bc
1a03b0020ead9bbf5d03761cddb929fa
2e2e21875ad473bd71ff3d32b405ada3
0ad71b4f28064748b22f3853ec544402

Pony:

mystoredoc[.]com/gate.php
sestoreinv[.]com/gate.php
menstoreins[.]com/gate.php
cukierniacapri[.]pl/wp-content/plugins/cached_data/m1.exe
cyctechnology[.]com/wp-content/plugins/cached_data/m1.exe
curatedayton[.]com/wp-content/plugins/cached_data/m1.exe
manydocsfastrack[.]com/gate.php
invoiceformater[.]com/gate.php
doclibrarymk[.]com/gate.php
en[.]beyoglugida[.]com/wp-content/plugins/cached_data/n1.exe
encentivhealth[.]com/wp-content/plugins/cached_data/n1.exe
en[.]inbar-solar[.]com/wp-content/plugins/cached_data/n1.exe
en[.]kotmed[.]com/wp-content/plugins/cached_data/n1.exe
essera[.]com/wp-content/plugins/cached_data/n1.exe
etc-coop[.]com/wp-content/plugins/cached_data/n1.exe
etc-ops[.]com/wp-content/plugins/cached_data/n1.exe
everylifecoach[.]org/wp-content/plugins/cached_data/n1.exe
docscountry[.]com/gate.php
sampledocstrash[.]com/gate.php
manterinvoice[.]com/gate.php
diamondlogosacademy[.]org/wp-content/plugins/cached_data/w2.exe
dierenkliniekpendrecht[.]nl/wp-content/plugins/cached_data/w2.exe
discoverbalaton[.]com/wp-content/plugins/cached_data/w2.exe
dev[.]mariocorp[.]com/wp-content/plugins/cached_data/w1.exe
dev[.]wbiz[.]it/wp-content/plugins/cached_data/w1.exe
diamondnailsvalpo[.]com/wp-content/plugins/cached_data/w1.exe
titanikvmoskalii[.]com/gate.php
toldronher[.]com/gate.php
tumanvmoskalii[.]com/gate.php
atolyedunyam[.]com/wp-content/plugins/feedweb_data/k1.exe
infogranizo[.]es/wp-content/plugins/feedweb_data/k1.exe

kinesis-gym[.]gr/wp-content/plugins/feedweb_data/k1.exe
servo-maszyny[.]pl/ADM/utility/tiny_mce/plugins/searchreplace/k1.exe
www.advisorz[.]co[.]uk/wp-content/plugins/feedweb_data/k1.exe
www.impulsos[.]net/wp-content/plugins/feedweb_data/k1.exe
leftofttarigh[.]ru/gate.php
undugdaid[.]ru/gate.php
lerecofrom[.]ru/gate.php
camemart[.]com/win.exe
akshajcreation[.]com/media/system/win.exe
digipillar[.]com/media/system/win.exe
wicytergo[.]ru/gate.php
unlaccothe[.]ru/gate.php
thetedrenre[.]ru/gate.php
eextensions[.]co/host.exe
www.10203040[.]at/host.exe
www.eshtari[.]me/host.exe
wicytergo[.]ru/sliva/gate.php
unlaccothe[.]ru/sliva/gate.php
thetedrenre[.]ru/sliva/gate.php
eextensions[.]co/m.exe
www.10203040[.]at/m.exe
www.eshtari[.]me/m.exe
dethetear[.]ru/gate.php
fortformares[.]ru/gate.php
tonslachesand[.]ru/gate.php
writeonlabels[.]biz/media/system/h1.exe
aultomax[.]com[.]au/h1.exe
sauvarinsglass[.]co[.]nz/h1.exe
dethetear[.]ru/sliva/gate.php
fortformares[.]ru/sliva/gate.php
tonslachesand[.]ru/sliva/gate.php
writeonlabels[.]biz/media/system/m.exe
aultomax[.]com[.]au/m.exe
sauvarinsglass[.]co[.]nz/m.exe
hagurowrob[.]ru/gate.php
betrewhattit[.]ru/gate.php
botepetan[.]ru/gate.php
www.raveshia[.]com/wp-content/plugins/cached_data/print.exe
elfielatorestaurante[.]com/wp-content/plugins/cached_data/print.exe
spiceone-food[.]com/wp-content/plugins/feedweb_data/print.exe
rewthenperhed[.]ru/gate.php
littmahedtbo[.]ru/gate.php
hedtheresran[.]ru/gate.php
guedesrusso[.]com/system/logs/print.exe
noshykart[.]com/system/logs/print.exe
php9[.]650mb[.]com/wp-content/plugins/cached_data/print.exe
buthimetrab[.]com/zapoy/gate.php
ughtotdinghar[.]ru/zapoy/gate.php

gebiketo[.]ru/zapoy/gate.php
retoftontto[.]com/zapoy/gate.php
hididnjustha[.]ru/zapoy/gate.php
hinjuskinuse[.]ru/zapoy/gate.php
buloftoty[.]com/zapoy/gate.php
soonbito[.]ru/zapoy/gate.php
letatandone[.]ru/zapoy/gate.php
wasscaltontuld[.]com/zapoy/gate.php
hemorananing[.]ru/zapoy/gate.php
ontedrirop[.]ru/zapoy/gate.php

f5efd86c80538e104503c309e458efa9
4ed1786f75251376f23bc0df2cd98fff
c1bfbfe0db4a74611e32cc7f49cc9383
379c67ae879872d3fa0b601892c59605
8c62d43ee165859603c532beecdbadde
be1f62fcbe151ad251a3a8d1d0d8b5e3
121cc78adcf9097b51813fbdbe0f4872
cd445e52eb7d2ca7359a8513157dd0a9
5e49ae017af49f89b2d7cc986677a266
0f7fd85685e7835fee897f2ab36652ac
896908f5cb3c8e045eb45c367f7cfdd6
b6226b00ea36f50d855e8c6da147b5c1
4e88d4d6ad6d581ec37c3597f6db8019
3e7541a41b84046e4994f660bda5dadc
3bfc4c70be70456d607c7fdc054f7252

H1N1:

britecompanies[.]com/pm.dll
britecompanies[.]com/inst1.exe
buthimetrab[.]com:80/h/gate.php
ughtotdinghar[.]ru:80/h/gate.php
gebiketo[.]ru:80/h/gate.php
retoftontto[.]com:80/h/gate.php
hididnjustha[.]ru:80/h/gate.php
hinjuskinuse[.]ru:80/h/gate.php
quonigeria[.]com/pm.dll
Ungr[.]net/inst.exe
crr-medvezonok[.]ru/about/inst3.exe
crr-medvezonok[.]ru/about/inst1.exe
crr-medvezonok[.]ru/about/inst2.exe
crr-medvezonok[.]ru/about/pm.dll
ontedrirop[.]ru/h/gate.php
hemorananing[.]ru/h/gate.php
wasscaltontuld[.]com/h/gate.php

4d0829e6c17c127d37a6ac6417787504

H1N1 DocDroppers:
B8b13f5b9fb54017b3a4b54cb0fc97c4
1265be272d9f4d37f34c0702c6841fb2

Nymaim:

162.244.32.157:8458 – Gozi Module BackConnect Server
oxrdmfdis[.]in/deip7/index.php
oxrdmfdis[.]in/awxCAe1jyu/index.php
xnkhfbc[.]in/qzlshd9xfv/index.php

ae4145a0a4859d5ab56b143adb148ee9
90e4d03aff298fca4641acda4e6493f2
4cadf61e96c2d62292320c556fd34fe6

Andromeda:

secure.adnxs.metalsystems[.]it/new_and/state.php
upfd.pilenga[.]co[.]uk/new_and/state.php
37.59.66.231/js/calc[.]pack
www.amicimusica.ud[.]it/audio/js.mod
antoniocaroli[.]it/prova/sd/LnMSLFOfwwout.exe

96daa23d7723f8f04690bb93642a9bae
f983ba24d259b4afac4451f7036e7636f6a35df175c6f7302e309ea7daab45ab

Andromeda RC4 key:
15ed0db7475d3c93e06a3677c194f855

ISFB/Gozi:

goyanok[.]at/krp3cmg/images/
outaplaceshave[.]cn/krp3cmg/images/
noopex[.]at/krp3cmg/images/
hothegivforsuffer[.]cn/krp3cmg/images/
lopertopgo[.]su/krp3cmg/images/
nexpoo[.]at/krp3cmg/images/
pergozip[.]at/krp3cmg/images/
justiceseasfriends[.]cn/krp3cmg/images/
mid100[.]at/krp3cmg/images/
goinumder[.]su/krp3cmg/images/
trepeatedandequal[.]cn/krp3cmg/images/
hulivam[.]at/krp3cmg/images/
therepalon[.]su/krp3cmg/images/
creatortherefore[.]cn/krp3cmg/images/

797717b96a3422d27b68365b4d54ebe9568b7b705d31bdc745f72b40b778c1bb

Dyre:

nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua[.]b32[.]i2p:443

```
62.122.69.172:4443
91.238.74.70:443
181.189.152.131:443
194.28.190.183:443
91.238.74.70:443
62.122.69.172:4443
181.189.152.131:443
194.28.190.183:443
95.67.88.84:4443
176.56.24.229:443
178.136.123.22:443
91.194.239.126:4443
94.231.178.46:4443
194.28.190.167:443
80.234.34.137:443
213.111.243.60:4443
46.149.253.52:4443
37.57.101.221:4443
134.249.63.46:443
85.192.165.229:443
195.34.206.204:443
62.122.69.159:4443
188.123.34.203:443
178.18.172.215:4443
91.232.157.139:443
195.206.255.131:443
37.232.185.114:443
62.182.33.16:443
46.180.147.50:443
46.175.23.130:443
84.16.54.22:443
84.16.55.122:443
93.184.71.88:4443
83.168.164.18:443
212.89.237.65:443
176.109.58.78:443
212.37.81.96:4443
95.165.196.227:443
195.34.239.93:443
77.234.235.48:443
217.12.59.238:443
212.62.58.238:443
212.69.14.89:443
195.206.254.15:443
46.167.219.231:443
31.28.115.88:443
62.122.69.137:4443
84.16.55.12:443
```

```
62.122.69.151:4443
194.28.190.84:443
194.28.190.146:443
194.28.191.144:443
194.28.191.213:443
213.87.54.111:443
213.87.54.111:443
46.16.111.158:443
31.41.90.230:4443
158.255.255.87:4443
109.195.2.150:443
88.208.22.210/30.su3
senyuplastics[.]com/75462354.txt
senyuplastics[.]com/lns.txt
91.194.254.235/uss/file.exe
91.194.254.222/us2/file.exe
77.85.204.114:443
194.28.190.99:443
194.28.190.88:443
94.180.109.121:443
194.28.190.86:443
91.242.53.142:4443
85.66.249.207:443
194.12.117.68:443
62.122.102.105:443
46.151.48.149:443
78.109.34.34:443
89.189.174.40:443
46.151.49.128:443
46.151.48.97:443
89.250.145.129:443
188.123.34.192:443
46.151.48.184:443
5.255.166.200/0.su3
87.116.153.216:443
176.120.201.9:443
80.87.219.35:443
31.42.170.118:443
91.240.97.141:443
93.91.154.243:443
184.164.97.60:443
77.95.192.36:443
178.22.222.89:443
67.207.228.144:443
69.9.204.37:443
84.237.229.49:443
217.23.194.237:443
107.161.199.59:4443
```

```
67.206.96.30:443
67.219.166.113:443
77.104.206.150:443
178.219.10.23:443
75.134.44.251:443
188.255.241.22:4443
67.206.97.238:443
69.146.233.162:4443
69.118.144.195:4443
188.255.236.227:4443
38.124.169.163:4443
185.31.33.98:443
95.143.131.73:443
46.37.205.163:443
41.75.67.80:443
41.75.68.226:443
41.75.68.242:443
41.215.182.109:443
46.44.28.44:443
78.8.174.25:443
78.58.131.116:443
118.179.219.210:443
132.255.212.105:443
150.129.49.11:443
154.73.140.26:443
176.106.122.32:443
178.168.109.92:443
179.49.117.33:4443
181.143.49.146:443
181.143.223.10:443
181.174.76.17:4443
190.111.20.50:443
193.189.77.76:443
196.2.10.17:443
197.231.198.234:4443
212.109.14.145:443
217.30.78.174:443
185.46.217.70:443
41.191.118.234:443
41.75.67.249:443
41.77.130.160:443
41.203.118.202:443
62.233.252.206:443
62.233.252.247:443
83.241.176.230:4443
91.232.45.149:443
109.196.1.13:4443
154.73.100.124:443
```

172.242.228.68:4443
173.185.166.94:4443
173.252.50.124:4443
186.42.215.214:443
186.46.185.174:443
190.63.152.74:443
190.151.95.243:443
190.215.141.163:443
197.254.104.166:4443
201.187.95.250:443
203.189.148.116:443
212.182.101.2:4443
93.126.47.107:443
46.143.196.142:443
31.40.1.32:443
87.248.158.109:443
107.181.174.68:443
107.181.174.68:443
185.49.68.145:4443
51.254.98.180:443

88ed077e12a8109933472ce6ca6a0296
ddebcf8183b9b8082a016aa646f899bb
46d84fb13afaab16b15322e52cd73b48
d6c0e93fce69f0e16ef11bc2e285be55

MacroDocs:
bankruptcy-software[.]com/wp-content/themes/classic/1.php?r
91.194.254.213/us/file.jpg
penis-enhancement-secrets[.]com/wp-content/plugins/lns.txt
peakperformancelifestyle[.]com/wp-content/plugins/lns.txt
penis-enhancement-secrets[.]com/wp-content/plugins/6612536153.txt
peakperformancelifestyle[.]com/wp-content/plugins/6612536153.txt
91.194.254.80/us705/file.exe
senyuplastics[.]com/75462354.txt
senyuplastics[.]com/lns.txt
91.194.254.235/uss/file.exe
91.194.254.222/us2/file.exe
capehilldentalsurgery[.]co[.]uk/wp-admin/includes/89172387.txt
brianlonchar[.]com/home/wp-includes/fonts/89172387.txt
capehilldentalsurgery[.]co[.]uk/wp-admin/includes/lns.txt
brianlonchar[.]com/home/wp-includes/fonts/lns.txt
carallianz[.]com/boilerd/keys/pa.exe
modern7technologiesx0[.]tk/x1656/dfiubgh5.exe
forbiddentextmate58[.]tk/x1656/ctruiovy.exe
temporary777winner777[.]tk/x1656/fdgbh44b.exe
former12futuristik888[.]tk/x1656/fdgjbhis75.exe
mehmetcanta[.]com/system/logs/office.exe

e763e99edac813ba6161c5545229cb34
0c98a7e39b0d9a0cb338faee3901182b
0c1f3d79559e261c4b60a76f665c364d
0cfd0039a3b9781e52c9b86c584da04a
8211ae4365f96c48a35619482fa7842d
a19cba9a758aff2d773c68cc42131fd3
b41205f6aeeeb1aa1fd8e0dcbddf270e

Older man1.exe from 20Jun2016:
4c4b2817873e0ae17cd05b7bd233d201

EmailLinks:

dovepersonnel[.]com[.]au/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
easydash[.]com[.]br/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
duvertepetasiyicilar[.]com/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
eciusda[.]org/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
dogadateknoloji[.]com/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
ecghouston[.]org/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
dutcharchitects[.]info/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
einkubator[.]com/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
dnacomvisual[.]com[.]br/wp-content/plugins/cached_data/aa_ticket_8392051302.zip
dodoty[.]com/wp-content/plugins/cached_data/aa_ticket_8392051302.zip
ogadateknoloji[.]com/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
dugunorganizasyonu[.]co/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
dymacorp[.]com/wp-content/plugins/cached_data/aa_ticket_9017937910.zip
djasad[.]co[.]uk/wp-content/plugins/cached_data/aa_ticket_8392051302.zip
dj-collision[.]com/wp-content/plugins/cached_data/aa_ticket_8392051302.zip
docitachocolates[.]com[.]br/wp-content/plugins/cached_data/aa_ticket_8392051302.zip
joetradeco[.]com/images/poultry/large/aa_ticket_8392051302.zip
drmuratcaglayan[.]com/wp-content/plugins/cached_data/aa_ticket_9017937910.zip

Dalexis:

ofigesvi[.]es:80/modules/history.jpg
pbescastell[.]es:80/pcss/history.jpg
onlinecomputer[.]at/wp-includes/history.jpg
artesanjuan[.]es/SpryAssets/history.jpg
mondoclinicsistem[.]ro/[.]htpasswds/history.jpg
www186[.]e1007[.]servidornet[.]com/wp-admin/history.jpg
pensiunea-lamuncel[.]ro/history.jpg
procosta[.]es/history.jpg
pensiunituristicebucovina[.]ro/pensiunea-lamuncel[.]ro/history.jpg

35096228e2d6e644cdd51259dcdaf03d

CTB-Locker:

3fdzgtam4qk625n6[.]tor2web[.]blutmagie[.]de

cbde2e916ae7accb98bb247bb93846c9

ReactorBot:

rc7thuhy8agn43zzgi[.]biz
heckwassleftran[.]ru
heckwassleftran2[.]ru
heckwassleftran3[.]ru
zdnuohzdydlpx5kd[.]onion
heckwassleftran[.]ru/cgi-bin/050515/post[.]cgi
heckwassleftran[.]ru/host[.]dat
heckwassleftran[.]ru/101/list32[.]dat
heckwassleftran[.]ru/101/1880376902_32[.]dat
heckwassleftran[.]ru/101/3257F7F8
heckwassleftran[.]ru/101/EB4E2654
heckwassleftran[.]ru/101/B06139B1

eff29f0ba620760a42c1ac0514007bff
3f11c42687d09d4a56c715f671143a58

P2P Gozi variant:
4e3a0ce170d66eaea6d55a3d6c551653

Nymaim Gozi Module Targets:

https://*pib*[.]secure-banking[.]com/*
https://www[.]svbconnect[.]com/auth*
https://connect-ch*[.]ubs[.]com/workbench/*
https://clientlogin[.]ibb[.]ubs[.]com/login*
https://achieveaccess[.]citizenscommercialbanking[.]com/CitizensWebApplication/achieve/loginScreen*
https://onlinebusinessplus[.]vancity[.]com/business/default[.]jsp*
https://www[.]vancity[.]com/BusinessBanking*
https://cashmanageronline[.]bbt[.]com/auth/*

```
https://onepass[.]regions[.]com/*
https://commerceconnections[.]commercebank[.]com/*
https://pfo[.]us[.]hsbc[.]com/*
https://*/fi*/bb/logon*
https://www8[.]comerica[.]com*
https://connect[.]bnymellon[.]com/ConnectLogin/login/LoginPage[.]jsp*
https://wellsoffice[.]wellsfargo[.]com/portal/signon/index[.]jsp*
https://*[.]ibanking-services[.]com/*
https://*LoginAdv[.]aspx*
https://*ebanking-services[.]com/EamWeb*
https://*/wcmfd/wcmpw/*
https://*phcp/servlet*
https://*[.]blilk[.]com/Core/Authentication/*
https://*1961/*1961[.]ashx*
https://*AOP/Password[.]aspx*
https://*ally[.]com*
https://*cm[.]netteller[.]com/login2008/Authentication*
https://securentrycorp*/Authentication/zbf/k/*
https://*/onlineserv/CM/*
https://*tob/live/usp-core/app/initialLogin*
https://*/CLKCCM/*/login[.]asp*
https://*/Authentication/Login[.]aspx*
https://*engine/login/logins*[.]asp*
https://*myebanking[.]net*
https://*hbloginv50*
https://*User/AccessSignin/*
https://drob[.]santanderbank[.]com/*
https://*bnymellonwealthmanagement[.]com*
*businessonline[.]tdbank[.]com/corporatebankingweb/core*
https://express[.]53[.]com/portal/auth/login/Login*
https://express[.]53[.]com/portal/auth/login/Login*
*/ibanking3/login[.]aspx*
https://trz[.]tranzact[.]org/LogonOTP[.]aspx
https://login[.]tranzact[.]org/account/login*
https://access[.]jpmorgan[.]com/jpmalogon*
https://jpmcsso[.]jpmorgan[.]com/sso/action/federateLogin*markets[.]jpmorgan[.]com*
https://jpmcsso[.]jpmorgan[.]com/sso/action/login*mdcommercial[.]jpmorgan[.]com*
https://cashproonline[.]bankofamerica[.]com/AuthenticationFrameworkWeb/cpo/login/public/loginMain[.]faces*
https://businessaccess[.]citibank[.]citigroup[.]com/cbusol/signon[.]do*
https://www[.]treasury[.]pncbank[.]com/idp/esec/login[.]ht*
https://singlepoint[.]usbank[.]com/cs70_banking/logon/sbuser*
```

https://*/cmserver/welcome/*
https://*engine/login/businesslogin[.]asp*
https://*/engine/login/businesslogins[.]asp*
https://*/pub/html/login[.]html*
https://ktt[.]key[.]com/ktt/cmd/logon*
https://*secure[.]fundsxpress[.]com/*
https://banamexusa[.]btbanking[.]com/onlineserv/CM/