SharkFest '16

Detection & verification of IoCs

Wednesday, June 15, 2016

Jasper Bongertz
Expert Analyst | Airbus Defence and Space CyberSecurity

Agenda

- The Incident Haystack
- Network Forensics
- Snort & Suricata
- TraceWrangler
- Wireshark

The Incident Haystack

- In an incident response situation at least one Indicator of Compromise has been found already
- The haystack is all of the IT infrastructure that needs to be checked:
  - Clients
  - Servers
  - Network
  - ISP uplinks

Looking for the Needle

- The problem
  - Telling what systems have really been compromised
- So how do we usually do that? Looking at
  - file systems
  - log files
  - firewall rule tables
  - sensor hits (IDS/IPS/NSM/AV/Sandboxes)
  - documentation

Looking at the Network

- Network forensics can be an effective way to spot potential „Needles“
- No matter how good malware hides, it‘ll use the network sooner or later
  - „No place to hide“ if sniffing packets at the right spot
- Problems:
  - Sniffing packets at the „right spot“
  - Scanning through gazillions of packets, looking for IoCs

Food for thought…

```
Public Sub fAnti6()
    Dim TimeNow As Long
    Dim TimeAfterSleep As Long
    TimeNow = GetTickCount
    Sleep 500
    TimeAfterSleep = GetTickCount
    If TimeAfterSleep - TimeNow < 500 Then End
End Sub

Public Sub fAnti7()
    Call fVerProceso("Wireshark.exe")
    Call fVerProceso("Xns5.exe")
    Call fVerProceso("wireshark.exe")
    Call fVerProceso("xns5.exe")
    Call fVerProceso("WireShark.exe")
    Call fVerProceso("smsniff.exe")
    Call fVerProceso("PROCEXP.exe")
End Sub
```

```
Private Sub fVerProceso(Proceso As String)
    On Error Resume Next
    Dim xProc, sInicio

    sInicio = "winmgmts://" & ""

    For Each xProc In GetObject(sInicio).InstancesOf("win32_process")
        If UCase(xProc.Name) = UCase(Proceso) Then End
    Next
End Sub
```

How did I find this script? Pastebin.

PASTEBIN + new paste trends API tools faq deals search...

My Alerts

You are allowed to add up to 15 alert keywords to your account. Whenever anyone creates a new public paste which matches your alert keywords, you will be instantly notified via email.

Email Address:

Keyword 1: | 0 emails sent | remove keyword

Keyword 2: | 0 emails sent | remove keyword

Keyword 3: | 1 emails sent | remove keyword

Keyword 4: | 1 emails sent | remove keyword

Keyword 5: | 0 emails sent | remove keyword

Keyword 6: | 0 emails sent | remove keyword

Keyword 7: | 0 emails sent | remove keyword

Keyword 8: | 0 emails sent | remove keyword

Keyword 9: Wireshark | 107 emails sent | remove keyword

Sniffing at the right spot

- Wireshark on a system may not be a good idea
  - in addition to the usual reasons it may be detected by malware
- SPAN ports are okay-ish
- Using TAPs is recommended
  - Packets have no place to hide when recorded correctly this way

Internet Uplinks

- Looking at Internet uplinks
  - Usually there are only a couple of them
- Problems:
  - "special purpose" DSL networks
  - undocumented uplinks
  - “rogue“ uplinks

Inspecting DNS traffic

- Can be stored a long time, e.g. using PassiveDNS
- Finding CnC patterns:
  - Answers containing Loopback addresses
  - High amount of errors like „no such name“
  - Domain Generation Algorithms
- Still need to sort out false positives
  - e.g. Loopback addresses as SPAM check results against Blacklists

DGA Example

- This is how Domain Generation Algorithm FQDNs may look like:

No.	IF ID	Source	Destination	Protocol	Info
6	0	192.168.100.227	192.168.100.1	DNS	Standard query 0x0566 A lubingindia.com
8	0	192.168.100.1	192.168.100.227	DNS	Standard query response 0x0566 A lubingindia.com A 50.23.73.100
570	0	192.168.100.227	192.168.100.1	DNS	Standard query 0xd667 A www.google.com
571	0	192.168.100.1	192.168.100.227	DNS	Standard query response 0xd667 A www.google.com A 173.194.112.17 A 173.194.1…
581	0	192.168.100.227	192.168.100.1	DNS	Standard query 0x6260 A www.google.de
583	0	192.168.100.1	192.168.100.227	DNS	Standard query response 0x6260 A www.google.de A 173.194.112.24 A 173.194.11…
632	0	192.168.100.227	192.168.100.1	DNS	Standard query 0x7061 A qshyvcjbpsgrsvkjffuufpr.biz
633	0	192.168.100.1	192.168.100.227	DNS	Standard query response 0x7061 A qshyvcjbpsgrsvkjffuufpr.biz A 67.215.65.132
642	0	192.168.100.227	192.168.100.1	DNS	Standard query 0x5363 A guidetest.a.id.opendns.com

Additional Measures

- Leveraging NetFlow
  - Long term storage of metadata of communication flows
  - Helps tracking lateral movement of attackers and building timelines
  - Can also be used for event correlation
- Baselining suspicious systems
  - Record everything it does
  - Using SPAN ports/TAPs
  - Pinpoint assets that require file system forensics

Verifying IoC Hits

Procedures

- First, you need to generate hits
  - for that, you need IoCs, e.g. in the form of Snort filters
- Steps involved:
  1. capture traffic
  2. run Snort against the pcaps
  3. grab resulting alert file / extracted frame pcaps
  4. verify in captured original pcaps
- The last step may take a loooong time when performed manually

Demo

Q&A

Mail: jasper@packet-foo.com
Web: blog.packet-foo.com
Twitter: @packetjay