


BfV Cyber-Brief Nr. 01/2018

- Hinweis auf aktuelle Angriffskampagne -



Kontakt:

Bundesamt für Verfassungsschutz
Referat 4D2/4D3

 0221/792-2600

Andauernde Bedrohung durch die Angriffe der APT¹ Berserk Bear auf deutsche Unternehmen

Dem Bundesamt für Verfassungsschutz (BfV) liegen Erkenntnisse über aktuelle Angriffe vor, die sich auch gegen deutsche Unternehmen richten. Die auf internationale Ziele ausgerichtete APT Berserk Bear – auch Energetic Bear, Crouching Yeti oder Dragonfly genannt – richtet ihre Angriffe zurzeit insbesondere gegen Unternehmen aus dem Energiesektor.

Sachverhalt

Angriffe und Aufklärungsaktivitäten, die der APT Berserk Bear zugerechnet werden, sind bereits seit mehreren Jahren bekannt. Im aktuellen Zielspektrum der Angreifer liegen vorwiegend KRITIS-Unternehmen (z.B. Energieversorgung, Wasserversorgung /-entsorgung, Informationstechnik/Telekommunikation). Dabei richteten sich die Angriffe der letzten Monate insbesondere gegen Infrastrukturkomponenten (z.B. Router). Die Angreifer verwenden vielfach öffentlich zugängliche Angriffswerkzeuge und versuchen unzureichend gesicherte Systeme unter ihre Kontrolle zu bringen.²

Um dies zu erreichen, scannen die Angreifer in der Regel in einem ersten Schritt einen Netzbereich mit potentiellen Opfern mit einem Portscanner, um einen Überblick über die Ports und Dienste zu erhalten, die offen vom Internet aus zu erreichen sind. Protokolle und Ports, die im Fokus des Angreifers stehen, sind unter anderem:

- Secure Shell (SSH, Port 22 TCP),
- Telnet (Telnet, Port 23 TCP),
- Hypertext Transport Protocol (HTTP, Port 80 TCP),
- Simple Network Management Protocol (SNMP, Port 161/162 UDP),
- Cisco Smart Install (SMI, Port 4786 TCP).

Neben möglichen Brute-Force-Angriffen auf die Fernwartungsprotokolle Telnet und SSH zwecks Erraten von Zugangsdaten senden die Angreifer SNMP- und SMI-Pakete mit entsprechenden Parametern an aktive Netzwerkkomponenten (z.B. Router) des Opfers. Falls Schutzmaßnahmen vor unbefugtem Zugriff wie Access Control Lists (ACL) auf den Komponenten konfiguriert wurden, werden die entsprechenden SNMP-Pakete mit gefälschten Absender-IP-Adressen versehen (IP-Spoofing, UDP Port 161), um die Schutzmaßnahmen zu umgehen.

Die an die Komponenten per SNMP oder SMI übermittelten Steuerbefehle veranlassen die Netzwerkkomponente, die aktuellen Konfigurationseinstellungen (u.a. die sog. running-config) an einen vom Angreifer kontrollierten Server via Trivial File Transfer Protokoll (TFTP) zu senden.

Die vom Opfer übermittelten Daten enthalten sensible Informationen u.a. zu der aktuellen Konfiguration, Modell, Hardware und Firmware des Routers, zur Infrastruktur des Netzwerkes und der Routingtabelle, zu freigegebenen Ports, Usernames und Passwörtern bzw. Hashwerten von Passwörtern.

¹ Advanced Persistent Threat.

² Am 16. April 2018 haben das Department of Homeland Security (DHS), das Federal Bureau of Investigation (FBI) und das National Cyber Security Centre (NCSC) gemeinsam eine Erklärung (US-CERT-Alert TA18-106A) veröffentlicht, die dieselbe APT betrifft.

In manchen Fällen wurden zudem unbefugte Änderungen an der Konfiguration der Netzwerkkomponenten vorgenommen, die zu einer Umlenkung von Datenverkehr über angreiferkontrollierte Systeme führten (GRE-Tunnel, Re-Routing). Dies ermöglicht den Angreifern das Auslesen und Manipulieren des umgeleiteten Netzwerkverkehrs (sog. Man-in-the-Middle-Angriff, kurz: MITM) sowie das Abschöpfen weiterer Zugangsdaten.

Als weiteren Angriffsvektor verwendet der Angreifer Spear Phishing Mails mit Anhängen oder vom Angreifer veränderte Webseiten, die einen sogenannten UNC-Verweis auf eine vom Angreifer kontrollierte, scheinbare Windows-Dateifreigabe enthalten (SMB³-Capture bzw. SMBTrap). Dies kann Windows-basierte Opfersysteme dazu veranlassen, den Benutzernamen und zugehörige Authentifizierungsdaten (NTLM-Hash) an das Angreifersystem zu übermitteln.

Die erbeuteten Login-Daten erleichtern es dem Angreifer, gegebenenfalls weitere Zugriffe auf das Opfernetzwerk über Remote-Services durchzuführen. Durch Verwendung legitimer Login-Daten fallen diese Zugriffe unter Umständen nicht sofort auf.

Handlungsempfehlung

Um festzustellen, ob Ihr Unternehmen von diesen Angriffen betroffen ist, empfehlen wir eine Durchsicht der Netzwerk-Logs auf

- ungewöhnliche Zugriffsversuche auf ggf. von außen erreichbare Telnet- und SSH-Dienste,
- unerwartete SNMP- bzw. SMI-Pakete,
- ungewöhnliche TFTP-Verbindungen mit Zielen außerhalb der eigenen Netzgrenzen sowie
- nach den in der Anlage aufgeführten Netzwerk-IOCs⁴.

Zudem sollte die Konfiguration der aktiven Netzwerkkomponenten auf unbefugte Änderungen, insb. die Einrichtung von ggf. ungewöhnlichen Tunnel-Einträgen (GRE) oder Routing-Einträgen geprüft werden.

Verwendete Software sollte stets auf dem neuesten Stand gehalten werden, damit dem Angreifer keine bekannten Sicherheitslücken geboten werden. Zusätzlich sollte neben rein präventiven Schutzmaßnahmen eine regelmäßige Erhebung und Prüfung von sicherheitsrelevanten Ereignissen erfolgen, um abnormales Verhalten im Netzwerk aufdecken zu können

Zur APT Berserk Bear existieren zusätzlich zahlreiche öffentliche Reports von IT-Sicherheitsunternehmen und Behörden. Zudem wurde bereits eine große Anzahl von IOCs zu Berserk Bear veröffentlicht. Daher werden in diesem Cyber-Brief lediglich die aktuellsten IOCs wiedergegeben.

Sollten Sie entsprechende Anhaltspunkte feststellen, besteht die Gefahr der Infizierung Ihrer Rechner. In diesem Fall können wir Ihre Maßnahmen mit zusätzlichen Hintergrundinformationen unterstützen und weitere Hinweise geben. Wir sichern Ihnen Vertraulichkeit zu. Hierzu stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung:

Tel.: 0221 - 792 - 2600 oder
E-Mail: poststelle@bfv.bund.de

³ SMB (Server Message Block) ist ein Netzwerkprotokoll für Datei- und Druckerfreigabe in Rechnernetzen. Es wird primär auf Betriebssystemen von Microsoft eingesetzt.

⁴ Indicators of Compromise

Wir weisen darauf hin, dass die Durchführung der in diesem Schreiben genannten Maßnahmen nicht die Meldung gemäß § 8b Abs. 4 BSI-Gesetz bzw. § 109 Abs. 5 TKG gegenüber dem Bundesamt für Sicherheit in der Informationstechnologie (BSI) ersetzt.

Empfehlung vorbeugender Maßnahmen

Als allgemeine vorbeugende Maßnahmen zum Schutz vor Infektionen empfehlen wir folgende Punkte zu beachten und diese auch den Beschäftigten Ihres Unternehmens in geeigneter Weise zur Kenntnis zu geben:

- Der Angreifer arbeitet mit kompromittierten E-Mail Adressen, sodass die Absender-Adresse und der Urheber der E-Mail legitim erscheinen können. Prüfen Sie eingehende E-Mails auf ihre Plausibilität, stellen Sie sich Fragen wie z.B. „Erwarte ich eine solche E-Mail? Ist der Kontext der E-Mail plausibel?“ Lassen Sie sich den Versand von ggf. ungewöhnlich erscheinenden E-Mails vom Absender bestätigen.
- E-Mails mit Anhängen und Links sollten grundsätzlich automatisiert in einer Analyseumgebung auf schädliches Verhalten geprüft werden.
- Deaktivieren Sie bei Netzwerkkomponenten (z.B. Router, Switches) nicht verschlüsselte Legacy-Protokolle wie z.B. Telnet, SNMPv1 oder SNMPv2c. Verwenden Sie nach Möglichkeit moderne verschlüsselte Protokolle wie SSH oder SNMPv3. Falls Sie Netzwerkkomponenten einsetzen, die lediglich veraltete Legacy-Protokolle unterstützten, sollten Sie diese möglichst zeitnah ersetzen.
- Lassen Sie keinen administrativen Zugriff auf Netzwerkkomponenten aus dem Internet zu. Beachten Sie jedoch, dass der Angreifer solche Schutzmaßnahmen mit gefälschten IP-Adressen gegebenenfalls umgehen kann. Falls ein Zugriff von außerhalb des lokalen Netzes notwendig ist, sollte der Remote-Zugriff über eine verschlüsselte VPN-Verbindung erfolgen.
- Durchsuchen Sie die Logdateien nach Datenverkehr, der an die Ports 23 TCP (Telnet), 161/162 UDP (SNMP) oder 4786 TCP (Cisco SMI) gerichtet ist. Prüfen Sie, ob die unten aufgelisteten netzwerk-basierten IOC in den Logdateien vorkommen.
- Durchsuchen Sie die Logdateien nach ausgehendem TFTP-Datenverkehr, der an das Internet gerichtet ist. Sollten Sie einen Zusammenhang zwischen eingehendem SNMP-Verkehr und kurz darauf folgendem ausgehenden TFTP-Verkehr finden, ist eine gründliche Analyse dieses Verkehrs empfehlenswert.
- Konfigurieren Sie Ihre Firewall entsprechend, sodass in das Internet ausgehender TFTP-Verkehr blockiert wird.
- Überprüfen Sie regelmäßig die Gerätekonfigurationen der Netzwerkkomponenten. Insbesondere sollte geprüft werden, ob es unbefugte Änderungen an Routingtabellen und Access Control Lists (ACL) gibt und ob ungewöhnliche GRE⁵-Tunnel eingerichtet wurden.
- Sperren Sie unerwünschten eingehenden Datenverkehr (aus dem Internet) und ausgehenden Datenverkehr (in Richtung Internet) auf den folgenden von SMB verwendeten Ports: 137-139, 445. Weitere Informationen zur sicheren Konfiguration von SMB finden Sie in den Richtlinien von Mi-

⁵ GRE (Generic Routing Encapsulation) ist ein Tunnelprotokoll, welches direkt auf IP (Internet Protocol) aufsetzt und die IP-Protokoll-Nummer 47 verwendet.

Microsoft für die Sperrung bestimmter Firewall-Ports, um zu verhindern, dass SMB-Datenverkehr die Unternehmensumgebung verlässt:

<https://support.microsoft.com/de-de/help/3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic>

Zusammenfassung von netzwerkbasieren IOC's:

US-CERT: Alert (TA18-106A) - Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices

<https://www.us-cert.gov/ncas/alerts/TA18-106A> (16.04.2018)

IP-Adressen:

176.223.111.160
210.245.123.180
80.255.3.85
87.120.41.3
91.207.57.69

Network Signatures:

Detect use of Cisco Smart Install (SMI):

The following signature may be used to detect SMI usage.

Flag as suspicious and investigate SMI traffic arriving from outside the network boundary.

If SMI is not used inside the network, any SMI traffic arriving on an internal interface should be flagged as suspicious and investigated for the existence of an unauthorized SMI director.

If SMI is used inside the network, ensure that the traffic is coming from an authorized SMI director, and not from a bogus director.

```
alert tcp any any -> any 4786 (msg:"Smart Install Protocol"; flow:established,only_stream; content:"|00 00 00 01 00 00 00 01|"; offset:0; depth:8; fast_pattern;)
```

See Cisco recommendations for detecting and mitigating SMI. ->

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi>

Detect use of Cisco Smart Install Exploitation Tool (SIET):

The following signatures detect usage of the SIET's commands `change_config`, `get_config`, `update_ios`, and `execute`.

These signatures are valid based on the SIET tool available as of early September 2017:

```
alert tcp any any -> any 4786 (msg:"SmartInstallExploitationTool_UpdateIos_And_Execute"; flow:established; content:"|00 00 00 01 00 00 00 01 00 00 00 02 00 00 01 c4|"; offset:0; depth:16; fast_pattern; content:"://";)
```


alert tcp any any -> any 4786 (msg:"SmartInstallExploitationTool_ChangeConfig"; flow:established; content:"|00 00 00 01 00 00 00 01 00 00 00 03 00 00 01 28|"; offset:0; depth:16; fast_pattern; content:"//");

alert tcp any any -> any 4786 (msg: "SmartInstallExploitationTool_GetConfig"; flow: established; content:"|00 00 00 01 00 00 00 01 00 00 00 08 00 00 04 08|"; offset:0; depth:16; fast_pattern; content:"copy|20");

US-CERT: Alert (TA18-074A) - Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

<https://www.us-cert.gov/ncas/alerts/TA18-074A> (15.03.2018)

IP-Adressen:

91.183.104.150

62.8.193.206

184.154.150.66

5.153.58.45

Network Signatures:

alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"HTTP URI contains '/aspnet_client/system_web/4_0_30319/update/' (Beacon)"; sid:42000000; rev:1; flow:established,to_server; content:"/aspnet_client/system_web/4_0_30319/update/"; http_uri; fast_pattern:only; classtype:bad-unknown; metadata:service http;)

alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"HTTP URI contains '/img/bson021.dat'"; sid:42000001; rev:1; flow:established,to_server; content:"/img/bson021.dat"; http_uri; fast_pattern:only; classtype:bad-unknown; metadata:service http;)

alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"HTTP URI contains '/A56WY' (Callback)"; sid:42000002; rev:1; flow:established,to_server; content:"/A56WY"; http_uri; fast_pattern; classtype:bad-unknown; metadata:service http;)

alert tcp any any -> any 445 (msg:"SMB Client Request contains 'AME_ICON.PNG' (SMB credential harvesting)"; sid:42000003; rev:1; flow:established,to_server; content:"|FF|SMB|75 00 00 00 00|"; offset:4; depth:9; content:"|08 00 01 00|"; distance:3; content:"|00 5c 5c|"; distance:2; within:3; content:"|5c|AME_ICON.PNG"; distance:7; fast_pattern; classtype:bad-unknown; metadata:service netbios-ssn;)

alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"HTTP URI OPTIONS contains '/ame_icon.png' (SMB credential harvesting)"; sid:42000004; rev:1; flow:established,to_server; content:"/ame_icon.png"; http_uri; fast_pattern:only; content:"OPTIONS"; nocase; http_method; classtype:bad-unknown; metadata:service http;)

alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"HTTP Client Header contains 'User-Agent|3a 20|Go-http-client/1.1'"; sid:42000005; rev:1; flow:established,to_server; content:"User-Agent|3a 20|Go-http-client/1.1|0d 0a|Accept-Encoding|3a 20|gzip"; http_header; fast_pattern:only; pcre:"/\.(?:aspx|txt)\?a-z0-9{3}=a-z0-9{32}&/U"; classtype:bad-unknown; metadata:service http;)

alert tcp \$EXTERNAL_NET 139,445 -> \$HOME_NET any (msg:"SMB Server Traffic contains NTLM-Authenticated SMBv1 Session"; sid:42000006; rev:1; flow:established,to_client; content:"|ff 53 4d 42 72 00 00 00 00 80|"; fast_pattern:only; content:"|05 00|"; distance:23; classtype:bad-unknown; meta-data:service netbios-ssn;)

GCHQ Advisory: Hostile state actors compromising UK organisations with focus on engineering and industrial control companies

https://www.ncsc.gov.uk/content/files/protected_files/article_files/NCSC%20advisory%20-%20CNI%20Supply%20Chain.pdf (05.04.2018)

IP-Adressen:

2.229.10.193
5.150.143.107
5.153.58.45
41.205.61.221
41.78.157.34
62.8.193.206
78.47.199.220
81.149.16.168
82.222.188.18
85.25.100.104
85.255.235.109
85.255.235.147
85.185.45.174
85.159.65.114
91.183.104.150
111.93.118.90
130.25.10.158
139.162.108.53
139.162.114.70
149.210.156.198
151.80.163.14
167.114.44.147
173.212.212.56
176.53.11.130
184.154.150.66
185.22.184.71
187.130.251.249
193.213.49.115
195.250.149.195
195.87.199.197
203.113.4.230

Dragonfly: Western energy sector targeted by sophisticated attack group

<https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks> (20.10.2017)

IP-Adressen:

103.41.177.69
37.1.202.26
184.154.150.66

Kaspersky Lab ICS CERT: Energetic Bear/Crouching Yeti: attacks on servers

https://ics-cert.kaspersky.com/media/EB_public_FINAL_EN_20042018.pdf (23.04.2018)

IP-Adresse:

155.207.63.4

Zusammenfassung von hostbasierten IOCs:

YARA

-> Quelle: Kaspersky 23. April 2018

```
rule Backdoored_ssh {
strings:
$a1 = "OpenSSH"
$a2 = "usage: ssh"
$a3 = "HISTFILE"
condition:
uint32(0) == 0x464c457f and filesize<1000000 and all of ($a*)
}
```

-> Quelle US CERT

```
rule APT_malware_1
{
meta:
description = "inveigh pen testing tools & related artifacts"
author = "DHS | NCCIC Code Analysis Team"
date = "2017/07/17"
hash0 = "61C909D2F625223DB2FB858BBDF42A76"
hash1 = "A07AA521E7CAFB360294E56969EDA5D6"
hash2 = "BA756DD64C1147515BA2298B6A760260"
hash3 = "8943E71A8C73B5E343AA9D2E19002373"
hash4 = "04738CA02F59A5CD394998A99FCD9613"
hash5 = "038A97B4E2F37F34B255F0643E49FC9D"
hash6 = "65A1A73253F04354886F375B59550B46"
hash7 = "AA905A3508D9309A93AD5C0EC26EBC9B"
hash8 = "5DBEF7BDDAF50624E840CCBCE2816594"
hash9 = "722154A36F32BA10E98020A8AD758A7A"
hash10 = "4595DBE00A538DF127E0079294C87DA0"
strings:
$s0 = "file://"
$s1 = "/ame_icon.png"
$s2 = "184.154.150.66"
$s3 = {
87D081F60C67F5086A003315D49A4000F7D6E8EB12000081F7F01BDD21F7DE }
```



```
$s4 = {
33C42BCB333DC0AD400043C1C61A33C3F7DE33F042C705B5AC400026AF2102 }
$s5 = "(g.charCodeAt(c)^(l[b]+l[e])%256)"
$s6 = "for(b=0;256>b;b++)k[b]=b;for(b=0;256>b;b++)"
$s7 = "VXNESWJfSjY3grKEkEkRuZeSvkE="
$s8 = "NlZzSZk="
$s9 = "WlJtb1q5kaxqZaRnser3sw=="
$s10 = "for(b=0;256>b;b++)k[b]=b;for(b=0;256>b;b++)"
$s11 = "fromCharCode(d.charCodeAt(e)^k[(k[b]+k[h])%256])"
$s12 = "ps.exe -accepteula \\%ws% -u %user% -p %pass% -s cmd /c
netstat"
$s13 = {
22546F6B656E733D312064656C696D733D5C5C222025254920494E20286C6973742E74787429
}
$s14 = {
68656C6C2E657865202D6E6F65786974202D657865637574696F6E706F6C696379206279706173
73202D
}
$s15 = {
476F206275696C642049443A202266626433373937623163313465306531 }
//inveigh pentesting tools
$s16 = {
24696E76656967682E7374617475735F71756575652E4164642822507265737320616E79206B657
920746
}
//specific malicious word document PK archive
$s17 = {
2F73657474696E67732E786D6CB456616FDB3613FEFE02EF7F10F4798E64C54D06A14ED125F19
A225E87
}
$s18 = {
6C732F73657474696E67732E786D6C2E72656C7355540500010076A41275780B00010400000000
040000
}
$s19 = {
8D90B94E03311086EBF014D6F4D87B48214471D210A41450A0E50146EBD943F8923D41C9DBE3
A54A240
}
$s20 = {
8C90CD4EEB301085D7BD4F61CDFEDA092150A1BADD005217B040E10146F124B1F09FEC01B56
F8FC3AA
}
$s21 = {
8C90CD4EEB301085D7BD4F61CDFEDA092150A1BADD005217B040E10146F124B1F09FEC01B56
F8FC3AA
}
$s22 = "5.153.58.45"
$s23 = "62.8.193.206"
```

```
$s24 = "/1/ree_stat/p"
$s25 = "/icon.png"
$s26 = "/pshare1/icon"
$s27 = "/notepad.png"
$s28 = "/pic.png"
$s29 = "http://bit.ly/2m0x8IH"
condition:
($s0 and $s1 or $s2) or ($s3 or $s4) or ($s5 and $s6 or $s7 and $s8 and
$s9) or ($s10 and $s11) or ($s12 and $s13) or ($s14) or ($s15) or ($s16) or ($s17)
or ($s18) or ($s19) or ($s20) or ($s21) or ($s0 and $s22 or $s24) or ($s0 and $s22
or $s25) or ($s0 and $s23 or $s26) or ($s0 and $s22 or $s27) or ($s0 and $s23 or
$s28) or ($s29)
}

{
meta:
description = "rule detects malware"
author = "other"
strings:
$api_hash = { 8A 08 84 C9 74 0D 80 C9 60 01 CB C1 E3 01 03 45 10 EB ED }
$http_push = "X-mode: push" nocase
$http_pop = "X-mode: pop" nocase
condition:
any of them
}
rule Query_XML_Code_MAL_DOC_PT_2
{
meta:
name = "Query_XML_Code_MAL_DOC_PT_2"
author = "other"
strings:
$zip_magic = { 50 4b 03 04 }
$dir1 = "word/_rels/settings.xml.rels"
$bytes = {8c 90 cd 4e eb 30 10 85 d7}
condition:
$zip_magic at 0 and $dir1 and $bytes
}

{
meta:
name = "Query_Javascript_Decode_Function"
author = "other"
strings:
$decode1 = {72 65 70 6C 61 63 65 28 2F 5B 5E 41 2D 5A 61 2D 7A 30 2D 39
5C 2B 5C 2F 5C 3D 5D 2F 67 2C 22 22 29 3B}
$decode2 = {22 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F 50 51 52 53
54 55 56 57 58 59 5A 61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73
74 75 76 77 78 79 7A 30 31 32 33 34 35 36 37 38 39 2B 2F 3D 22 2E 69 6E 64 65
```

```
78 4F 66 28 ?? 2E 63 68 61 72 41 74 28 ?? 2B 2B 29 29}
$decode3 = {3D ?? 3C 3C 32 7C ?? 3E 3E 34 2C ?? 3D 28 ?? 26 31 35 29 3C
3C 34 7C ?? 3E 3E 32 2C ?? 3D 28 ?? 26 33 29 3C 3C 36 7C ?? 2C ?? 2B 3D [1-2]
53 74 72 69 6E 67 2E 66 72 6F 6D 43 68 61 72 43 6F 64 65 28 ?? 29 2C 36 34 21
3D ?? 26 26 28 ?? 2B 3D 53 74 72 69 6E 67 2E 66 72 6F 6D 43 68 61 72 43 6F 64
65 28 ?? 29}
$decode4 = {73 75 62 73 74 72 69 6E 67 28 34 2C ?? 2E 6C 65 6E 67 74 68
29}
$func_call="a(\\"
condition:
filesize < 20KB and #func_call > 20 and all of ($decode*)
}

{
meta:
name= "Query_XML_Code_MAL_DOC"
author = "other"
strings:
$zip_magic = { 50 4b 03 04 }
$dir = "word/_rels/" ascii
$dir2 = "word/theme/theme1.xml" ascii
$style = "word/styles.xml" ascii
condition:
$zip_magic at 0 and $dir at 0x0145 and $dir2 at 0x02b7 and $style at 0x08fd
}

{
meta:
description = "Detection for the z_webshell"
author = "DHS NCCIC Hunt and Incident Response Team"
date = "2018/01/25"
md5 = "2C9095C965A55EFC46E16B86F9B7D6C6"
strings:
$aspx_identifier1 = "<%@" nocase ascii wide
$aspx_identifier2 = "<asp:" nocase ascii wide
$script_import = /(import|assembly) Name(space)?\=\\"(System|Microsoft)/
nocase ascii wide
$case_string = /case \"z_(dir|file|FM|sql)_/ nocase ascii wide
$webshell_name = "public string z_progname =" nocase ascii wide
$webshell_password = "public string Password =" nocase ascii wide
condition:
1 of ($aspx_identifier*)
and #script_import > 10
and #case_string > 7
and 2 of ($webshell_*)
and filesize < 100KB
}
}
```

Zusätzliche IOCs können Sie den oben genannten Berichten entnehmen.