Meldungstypen

Die im Rahmen des AW-Dienstes beobachteten Vorfälle sind unterschiedlicher Art. Zu diesem Zweck werden sie durch sogenannte Meldungstypen klassifiziert. Jeder Meldungstyp steht für eine Klasse von ähnlichen Vorfällen.

In den verschickten Warnmeldungen werden die Meldungstypen nur kurz erläutert, um die Warnmeldungen nicht zu lang werden zu lassen. Auf diesen Webseiten finden Sie ausführliche Erläuterungen zu allen Meldungstypen inklusive konkreter Beispiele.

Derzeit werden folgende Meldungstypen verwendet:

Attack

Bot

Command and Control Server

Configuration

Hosting

Scan

SPAM

Vulnerability

Neben der tabellarischen Darstellung im Textteil der Warnmeldung, beinhalten die E-Mails, die wir Ihnen schicken auch einen XML-Anhang, der sich insbesondere zur automatischen Verarbeitung der Warnmeldungen eignet.

Die Struktur dieses XML-Anhangs stellt sich etwas vereinfacht wie folgt dar:

```
<warning awId="AW#JJJJ-XXXXXXX>
  <message category="Meldungskategorie" ip="aaa.bbb.ccc.ddd">
    <description>Kurze Meldungserläuterung.
    </description>
    <event timestamp="Zeitpunkt der Beobachtung" ... >
      <auxiliary_info ... />
      <record>Textbeleg der Beobachtung</record>
    </event>
  </message>
</warning>
```

Die einzelnen Elemente dieser Meldung sind dabei

- message - Alle Meldungen einer Kategorie zu einer IP-Adresse. Dieses Element entspricht einemTabellenblock im Textteil der Warnmeldung. Kategorie und IP-Adresse finden sich in den Atributen dieses Elements.
- description - Die kurze Meldungserläuterung der Meldungskategorie. Diese entspricht der Erläuterung im Tabellenblock.
- event - Eine einzelne Beobachtung zu Kategorie und IP-Adresse. Diese enthält immer einen Zeitstempel (timestamp), der in der Regel mit dem "Zuletzt gesehen" Zeistempel im Textteil übereinstimmt.

Zusätzlich treten in Abhängigkeit von der Kategorie folgende Attribute auf:

  - **cert_diagnosis**: Name der diagnostizierten Malware
  - **feedback**: Link zu der Beobachtung bei der ursprünglichen Quelle. Dies dient zum Beispiel dazu Spamvorfälle bei der ursprünglichen Quelle als bearbeitet zu markieren und so ggf. Blacklisteinträge zu verhindern oder zu entfernen.
  - **ip_protocol**: IP-Protokoll der Beobachtung (TCP, UDP)
  - **malware_hash**: Hashsumme einer beobachteten Malware
  - **malware_hash_type**: Typ der Hashsumme (MD5, SHA1, ...)
  - **observation_end**: Ende der Beobachtungen. Werden mehrere Beobachtungen über einen gewissen Zeitraum aggregiert, so startet dieser Zeitraum mit dem Zeitstempel in timestamp und endet mit dem als observation_end angeführten Zeitstempel. In diesem Fall erscheint der observation_end Zeitstempel als "Zuletzt gesehen" im Textteil der Warnmeldung.
  - **occurences**: Anzahl der Beobachtungen. Werden mehrere Beobachtungen aggregiert, so gibt dies die Anzahl der aggregierten Beobachtungen an.
  - **request**: Beobachteter HTML-Request
  - **service**: Betroffener Dienst (SSH, FTP, ...)
  - **source_port**: Port auf dem betroffenen System
  - **source_url**: URL auf dem betroffenen System. Achtung: Modifikationen der URL, die zum Schutz vor versehentlichen Klicks vorgenommen werden (http durch hXXp ersetzen), werden im XML-Anhang nicht durchgeführt. Dies gilt auch für die später beschriebenen target_url und unknown_url.
  - **target_ip**: Vom betroffenen System kontaktierte IP-Adresse
  - **target_port**: Port auf dem kontaktierten System
  - **target_url**: URL auf dem kontaktierten System
  - **unknown_url**: Relevante URL. Diese kann sich sowohl auf dem betroffenen System als auch auf einem anderen System befinden.
- auxiliary_info - Liegen uns zu einer Beobachtung weitere Informationen vor, die üblicherweise nicht in einer Meldung dieser Kategorie enthalten sind, so werden diese als zusätzliches Element dem event hinzugefügt. Dabei werden die gleichen Attribute wie für das event verwendet. Das heißt, die üblicherweise vorhandenen Attribute einer Kategorie finden sich im event, sind zusätzliche Informationen verfügbar, finden Sie diese als Attribute in auxiliary_info. Die entsprechende Aufteilung wird in der tabellarischen Darstellung im Textteil der Warnmeldung vorgenommen.
- record - Liegt uns zu einer Beobachtung ein textueller Beleg vor, etwa die Header einer registrierten Spam-E-Mail, so werden diese in einem zusätzlichen Element dem event hinzugefügt. Dieses Element hat keine Attribute und beinhaltet direkt den textuellen Beleg der Beobachtung.

Beschreibung der Meldungstypen

Meldungstyp: Attack

Mit dieser Meldungskategorie versehen wir Angriffe, die von einem kompromittierten System aus durchgeführt werden. Diese werden häufig dadurch erkannt, dass das DFN-CERT und andere Organisationen sog. Honeypots betreiben. Dies sind Systeme, die einem Angreifer bestimmte Dienste vortäuschen, um ihn zu einem Angriff zu verleiten und so kompromittierte Systeme zu offenbaren. In diesen Fällen wurde der Versuch festgestellt, eine Schwachstelle auszunutzen. D. h. es handelt sich nicht nur um einen Portscan. Die Wahrscheinlichkeit einer Falschmeldung, d. h. dass ein System nur zufällig die Verbindungen aufgebaut hat, ist daher relativ gering.

Attack/Login

Ein Attack/Login ist ein Angriff, bei dem Angreifer versuchen, durch wiederholtes Ausprobieren von Passwörtern in ein System einzudringen.

Ein Attack/Login ist ein Angriff, bei dem Angreifer versuchen, durch wiederholtes Ausprobieren von Passwörtern in ein System einzudringen. Solche Angriffe sind vor allem bei den Diensten SSH, FTP, MS SQL und bei CGI-Anwendungen zu beobachten. Verbreitete Account-Namen und oft verwendete Passwörter liegen dabei als Listen vor und werden der Reihe nach durchprobiert. Der Angriff ist an vielen erfolglosen Anmeldeversuchen zu erkennen, die oft von Systemen erfolgen, die nichts mit dem Zielsystem zu tun haben. Diese Art des Angriffs wird auch Brute Force Angriff, Passwort-Rate Angriff oder Dictionary Attack genannt.

Im Folgenden sehen Sie ein typisches Beispiel:

```
Attack/Login
------------
Textteil:

IP-Adresse:   192.0.2.1
Meldungstyp:  Attack/Login
Zeitstempel:  2014-09-03 14:06:00+02:00
Anzahl:       2
Beschreibung: Das System hat einen Account Probe durchgeführt; d.h. es
              wurde wiederholt versucht, den Namen und das Passwort eines
              legitimen Benutzers zu erraten, um so Zugang zu fremden
              Systemen zu erlangen.

Zuletzt gesehen             Quellport          Ziel-IP    Zielport  Dienst
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
2014-09-03 14:05:23+02:00                                      22  SSH
2014-09-03 14:06:00+02:00                                      22  SSH

XML-Anhang:

<message category="Attack/Login" ip="192.0.2.1">
    <description>Das System hat einen Account Probe durchgefÜhrt; d.h. es
wurde
wiederholt versucht, den Namen und das Passwort eines legitimen Benutzers
zu
erraten, um so Zugang zu fremden Systemen zu erlangen.</description>
    <event timestamp="2014-09-03 14:05:23+02:00" target_port="22"
service="SSH"/>
    <event timestamp="2014-09-03 14:06:00+02:00" target_port="22"
service="SSH"/>
</message>
```

Attack/Malware

Schadsoftware verbreitet sich häufig, indem sie nach bestimmten Diensten sucht, um dann potentielle Schwachstellen in diesen Diensten auszunutzen. Ist dies erfolgreich, überträgt sich die Schadsoftware auf das frisch kompromittierte System. Zur Erkennung werden Honeypots eingesetzt, die verschiedene Dienste vortäuschen und versuchen, die Schadsoftware in dem Glauben zu lassen, dass eine Schwachstelle erfolgreich ausgenutzt wurde. Je nachdem wie weit der Angriff erfolgreich war, stehen bestimmte Informationen zur Verfügung. Es können die Suche nach einem angreifbaren Dienst erkannt oder angegriffene Ports identifiziert werden. Evtl. wird sogar die eigentliche Schadsoftware übertragen. Das DFN-CERT testet die Schadsoftware dann mit verschiedenen Virenscannern, um diese zu identifizieren. Dabei werden die Hashsumme und der ermittelte Name angegeben.

Im Folgenden sehen Sie ein typisches Beispiel. Dieses enthält zwei verschiedenartige Einträge in der Tabelle.

```
Attack/Malware
--------------

Textteil:

IP-Adresse:   192.0.2.5
Meldungstyp:  Attack/Malware
Zeitstempel:  2014-09-03 14:08:00+02:00
Anzahl:       2
Beschreibung: Das System fiel durch Angriffe auf Sensoren auf, bei denen
              Schadsoftware zum Download bereitgestellt wurde. Evtl. wird
              die Schadsoftware lediglich zum Download angeboten oder das
              System ist mit einem Virus infiziert, der die Schadsoftware
              jeweils zur Infizierung des nächsten Systems bereitstellt.

Zuletzt gesehen             Quellport    Zielport  Malware
Hashtyp  Hashsumme
------------------------------------------------------------------------------
2014-09-03 14:07:00+02:00       13763          21
MD5      72d1fd9a49ea2bd33476a5591a7a593c
2014-09-03 14:08:00+02:00
Trojan.BO2K.plugin.BlowFish.B


XML-Anhang:

<message category="Attack/Malware" ip="192.0.2.5">
    <description>Das System fiel durch Angriffe auf Sensoren auf, bei denen
Schadsoftware zum Download bereitgestellt wurde. Evtl. wird die
Schadsoftware
lediglich zum Download angeboten oder das System ist mit einem Virus
infiziert,
der die Schadsoftware jeweils zur Infizierung des nächsten Systems
bereitstellt.</description>
    <event timestamp="2014-09-03 14:07:00+02:00" source_port="13763"
target_port="21" malware_hash_type="MD5"
malware_hash="72d1fd9a49ea2bd33476a5591a7a593c"/>
    <event timestamp="2014-09-03 14:08:00+02:00"
cert_diagnosis="Trojan.BO2K.plugin.BlowFish.B"/>
</message>
```

Attack/Adware

Adware bzw. andere Software mit unerwünschten Funktionen (PUA) enthalten u. a. Funktionen zur Einblendung von Werbung, zum Klickbetrug (Click Fraud) oder können weitere Schadsoftware nachladen und ohne Zustimmung des Nutzers installieren. Da diese Art von Schadprogrammen zum Nachladen von Schadcode, zum Übermitteln von ausgespähten Informationen oder zum Empfangen von Instruktionen eine Verbindung zu einem Kontrollserver (C&C) aufnehmen, erfolgt die Detektion des Vorhandenseins einer solchen Software über die Sichtung solcher Verbindungen. Dabei werden die bekannten Domainnamen der Kontrollserver auf sogenannte Sinkholes umgeleitet, über welche die Auswertung erfolgt.

Attack/Amplifier

Offen aus dem Internet erreichbare UDP-basierte Dienste wie z. B. offene DNS-Resolver, NTP-Server mit aktiver 'monlist'-Funktion, offene SNMP-Server oder Portmapper können für DDoS-Reflection-Angriffe ausgenutzt werden, da diese Dienste auf Anfragen mit gefälschter Absenderadresse antworten und dabei Antworten die ein Vielfaches der Größe der Anfrage haben zurücksenden.

Attack/Credentials

Die Zugangsdaten eines E-Mail-Kontos sind bei der Übermittlung an einen Kontrollserver aufgefallen und sollten als kompromittiert angesehen werden.

Attack/Virus

Hierbei handelt es sich um eine vom DFN Mailsupport blockierte E-Mail, welche höchstwahrscheinlich Malware bzw. einen Virus enthält.

Attack/Phishing

Der Versand einer E-Mail, die vermutlich Phishing zum Zweck hatte, wurde blockiert.

Meldungstyp: Bot

Als Botnet wird eine Menge von kompromittierten Systemen (sogenannte Bots) bezeichnet, die sich vollständig unter der Kontrolle eines Angreifers befindet. Dies sind oft normale Arbeitsplatzrechner, in die über eine beliebige Schwachstelle eingebrochen wurde. Nach dem Einbruch wurde vom Angreifer eine Bot-Software installiert, die versteckt auf dem System läuft und eine Verbindung zu einem zentralen Botnet Control Server hält.

Wenn Sie eine Meldung bzgl. eines Bots bekommen, dann steht Ihr System wahrscheinlich unter der Kontrolle eines Angreifers und ist Teil eines Botnet. Booten Sie von einem sauberen Medium (z. B. CD) und untersuchen Sie dann das System.

Dieses ist evtl. am Versand von unerwünschter Werbemail beteiligt (SPAM) oder es werden Portscans oder gar Angriffe gegen weitere Systeme durchgeführt. Die Bots suchen auf dem kompromittierten System häufig auch nach Lizenzschlüsseln von Software (Spiele, Windows, Office), Passwörtern (für Homebanking, eBay, PayPal, etc.), betreiben Sniffer, Keylogger uvm.

Im Folgenden sehen Sie ein typisches Beispiel:

```
Bot/HTTP
--------

Textteil:

IP-Adresse:    192.0.2.21
Meldungstyp:   Bot/HTTP
Zeitstempel:   2014-09-03 14:12:00+02:00
Anzahl:        1
Beschreibung: Auf dem System scheint eine Bot-Software betrieben zu
              werden, die versucht, einen HTTP-basierten Bot-Netz Control-
              Server zu erreichen. Zu den unterschiedlichen Malwaretypen
              finden Sie unter der folgenden Webseite mehr Informationen:
              http://www.cert.dfn.de/index.php?id=bot

Zuletzt gesehen            IP-Protokoll   Quellport    Zielport  Malware
HTTP-Request
-------------------------------------------------------------------------
2014-09-03 14:12:00+02:00  TCP                22777          80  Conficker
GET /search?q=3164 HTTP/1.0


XML-Anhang:

<message category="Bot/HTTP" ip="192.0.2.21">
    <description>Auf dem System scheint eine Bot-Software betrieben zu
werden, die versucht, einen HTTP-basierten Bot-Netz Control- Server zu
erreichen. Zu den unterschiedlichen Malwaretypen finden Sie unter der
folgenden Webseite mehr Informationen:
http://www.cert.dfn.de/index.php?id=bot</description>
    <event timestamp="2014-09-03 14:12:00+02:00" ip_protocol="TCP"
source_port="22777" target_port="80" cert_diagnosis="Conficker"
request="GET /search?q=3164 HTTP/1.0"/>
</message>
```

Stehen uns detailliertere Informationen zum Beispiel über die Verbindung zum Botnet Control Server bereit, so reichen wir diese selbstverständlich an Sie weiter. Ein Beispiel dafür finden Sie hier.

Laufend aktualisierte Informationen zu der Schadsoftware Emotet finden Sie unter:

https://www.dfn-cert.de/aktuell/emotet-aktuell.html.

Malwaretypen

Die folgenden Malwaretypen werden derzeit unterschieden:

- Avalanche: Das System fiel auf, da es versuchte sich mit dem Avalanche Botnet zu verbinden. Avalanche verwendet Fast-Flux Domains um Phishing-Sites zu hosten. Der Bot ist in seinem Verhalten dem unten beschriebenen Zeus ähnlich.
- Conficker: Das System ist sehr wahrscheinlich mit dem Conficker Wurm (auch Downadup genannt) infiziert. Diese Malware verbreitet sich auf mehrere Arten im Netz und fällt durch HTTP-Anfragen der Form "http://<zufaellig_erzeugte_URL>" auf. Informationen zum Wurm und seiner Beseitigung finden Sie auf der Informationsseite von Microsoft oder auf der heise Security Infoseite.
- Conficker-Timecheck: Ab der Version C des W32.Conficker Wurms wird von Conficker eine Verbindung zu einer Reihe von öffentlichen Webservern aufgebaut, um die aktuelle Zeit abzufragen. Anhand dieser Anfragen können vom Wurm kompromittierte Systeme in den Logdateien der Webserver erkannt und ausgenutzt werden. Die Meldung "Conficker

Timecheck" besagt, dass sich ein System aus Ihrem Netzwerk zu einem dieser Server verbunden hat.

- Dipnet: Die Dipnet Bot-Software (auch Oddbob genannt) verwendet eine ältere LSASS-Schwachstelle, um sich zu verbreiten. Ist ein System infiziert, verbindet es sich zu einem privaten IRC-Server. Die Bot-Software führt Scans nach Port 15118/TCP durch, wodurch sie i. d. R. entdeckt wird.
- DNSChanger: Die Bot-Software DNSChanger verändert die DNS-Einstellungen des Computers so, dass Netzwerkverkehr auf von Angreifern kontrollierte Seiten umgeleitet wird. Beispiele hierfür sind Seiten von Banken oder generell Seiten auf denen Anwender Login-Daten eingeben. Weitere Informationen finden sie bei Heise Security oder in der Microsoft Malware Encyclopedia.
- FakeAV: Das gemeldete System ist durch den Zugriff auf FakeAV Server aufgefallen. Bei FakeAV, auch "rogue security software" genannt, handelt es sich um eine Anwendung, die vorgibt, eine legitime Sicherheitsanwendung wie z. B. ein Virenscanner oder Registry-Cleaner zu sein. Tatsächlich bietet sie jedoch keinen Schutz. In einigen Fällen wird zudem tatsächlich bösartige Software auf dem System installiert.
- Grum: Der Trojaner Grum wird üblicherweise zum Versenden von Spam eingesetzt. Das System fällt durch HTTP GET Requests "GET/spm/s_alive.php?" auf, die das Rootkit-geschützte Virus zu bestimmten URLs mit verschiedenen Parametern aufruft.
- Mariposa: Das System hat Verbindung zu einem bekannten "Command and Control"-Server des Mariposa-Botnetzes aufgenommen. Hierbei kann es sich sowohl um IRC- als auch HTTP-Verbindungen handeln. Ein System, das in dieses Botnetz eingebunden ist, kann für verschiedene kriminelle Zwecke verwendet werden, z. B. können Zugangsdaten für soziale Netzwerke, Online-Banking, FTP- oder E-Mailkonten gestohlen werden. Es gibt auch Berichte über "Distributed Denial-of-Service"-Angriffe mit diesem Botnetz.
- Mebroot: Das System ist durch HTTP POST Requests aufgefallen, die das Rootkit bzw. der davon geschützte Torpig Trojaner zu bestimmten URLs aufnimmt.
- Multibanker: Die Malware modifiziert Systemdateien, um Internetverkehr mit Bankwebseiten und ähnlichen Webseiten zu überwachen und die Logindaten zu stehlen. Diese Daten werden dann per HTTP an entfernte Rechner gesendet. Die Ziel-Adresse wird mittels eines dynamischen Algorithmus zur Erzeugung von Domainnamen aufgelöst. Weiterhin ist es möglich, dass weitere Schadsoftware heruntergeladen wird. Aliasnamen für die Malware sind unter anderem 'Bankpatch' und 'Multibanker'.
- Phatbot: Die Phatbot Bot-Software ist sehr modular und bietet Angreifern eine Vielzahl von Möglichkeiten sowie Exploits zur weiteren Verbreitung. Sie fällt durch bestimmte HTTP-Requests auf, die wahrscheinlich zur Bandbreiten-Messung an eine Reihe von Webseiten gerichtet werden. Da die Anfragen per HTTP gestellt werden, ist das System evtl. nur ein HTTP-Proxy und nicht das tatsächlich betroffene System.
- Sality: Das System hat eine Verbindung zu einer Download-URL des Sality Botnets aufgenommen. W32.Sality ist ein Bot, der sich über infizierte Dateien verbreitet. Neben der Infektion von Dateien und Prozessen erfüllt das Schadprogramm weitere Aufgaben. Es erschwert die Entdeckung des Programms durch Anti-Viren Software und lädt neue Komponenten nach. Ferner baut das Programm über ein eigenes Peer-2-Peer Protokoll Verbindungen zu anderen Instanzen auf. Ist ein System mit dem Sality-Bot infiziert, so öffnet das Programm auf dem Host eine Backdoor, welche einem Angreifer den Zugang zum System ermöglicht. Weiterhin werden Keylogger aktiviert, um die Aktionen des Anwenders zu protokollieren. Durch die Fähigkeit dynamisch Code nachzuladen, ist das System in der Lage, neue Funktionen zu integrieren.

- Sdbot: Die Bot-Software Backdoor.Sdbot verbreitet sich sowohl durch die Ausnutzung von Schwachstellen in Microsoft Windows als auch über offene SMB-Shares. Vermutlich wird dieser Bot auch entweder als Attachment an E-Mails verbreitet oder per Download von Webservern. Nach dem Starten des Bots verbindet sich dieser zu einem IRC-Channel des Angreifers und lässt sich so beliebig fernsteuern.
- Silon: Von dem System ausgehend wurde ein HTTP-Verbindungsversuch zu einem "Command and Control"-Server beobachtet. Der Trojaner Silon wird beispielsweise verwendet, um Login-Daten aus Sitzungen des Internet Explorers auszulesen und an zentrale Server zu schicken.
- sinit: Die Bot-Software sinit verwendet nicht IRC als Protokoll für den Control-Channel, sondern UDP Pakete auf Port 53, die fast wie DNS-Antworten aussehen. Weiterhin verwendet sinit ein dezentrales Peer-to-Peer Modell, um Befehle zu empfangen und zu verbreiten, was eine Aufdeckung relativ schwierig macht. Die Bot-Software fällt durch die Kommunikation auf Port 53/UDP auf.
- Spybot: Die Bot-Software W32.Spybot.WON benutzt eine Schwachstelle im Windows Plug-and-Play Interface zur weiteren Verbreitung.
- Spyeye: Die Bot-Software Spyeye zeichnet Keyboard-Aktivitäten auf und dient hauptsächlich dem Zweck, Login-Daten mithilfe einer Methode mit dem Namen "form grabbing" zu stehlen. Die Daten werden dann an einen entfernten Rechner geschickt. Die Malware verwendet dabei ein Rootkit, um ihre Aktivitäten zu verstecken.
- SSH-Brute-Forcer: Der Malwaretyp SSH-Brute-Forcer beschreibt eine Bot-Software, welche auffiel, da das befallene System SSH Account Probes auf anderen Systemen durchführte.
- Tdss: Die Bot-Software Tdss gehört zu einer Familie von Trojanern, die aus mehreren Komponenten besteht. Die Malware kann dabei Einfluss auf die Online-Aktivitäten des Rechners nehmen. Zum Beispiel kann sie Suchergebnisse manipulieren, auf bestimmte Seiten umleiten, sogenanntes Banner-Clicking ausführen oder unbemerkt Software herunterladen und installieren.
- Torpig: Der Torpig (auch Sinoval genannte) Trojaner wird zum Ausspähen von Bankverbindungen bzw. Usernamen und Passworten benutzt. Häufig wird die Anwesenheit des Trojaners durch das Mebroot Rootkit verschleiert.
- Toxbot: Die Bot-Software W32.Toxbot benutzt eine Vielzahl von Exploits, um sich weiter zu verbreiten. Ist ein System infiziert, versucht sich der Bot zu einem Botnet Control Server auf Port 6556/TCP oder 1023/TCP zu verbinden.
- TrafficConverter: Das System ist durch den Zugriff auf eine TrafficConverter Web-Adresse aufgefallen. TrafficConverter beschreibt eine internet-basierte Vertriebslösung (Affiliate-Program) für FakeAV Software. Den Affiliates werden Linkadressen und Javaskripte zur Verfügung gestellt, die in Software und kompromittierte oder bösartige Webseiten eingebunden werden können. Beim Zugriff auf diese Webseiten erscheinen irreführende Meldungen, die eine Infektion des Systems suggerieren und einen Gratis-Scan anbieten. Bei Zustimmung wird ein FakeAV Programm heruntergeladen, das vor nicht-existierenden Bedrohungen warnt. Zudem wird der Zugriff auf Webseiten legitimer Sicherheitsanbieter verhindert. Der Anwender wird daraufhin mit häufigen trügerischen Sicherheitsmeldungen dazu gedrängt, eine kostenpflichtige Version zu erwerben.
- Zeus: Vom System wurde zumindest ein HTTP-Verbindungsversuch zu einem "Command and Control"-Server des Zeus-Botnetzes registriert. Die Bots des Zeus-Netzes werden verwendet, um Zugangsdaten für soziale Netzwerke, Online-Banking, FTP- oder E-Mailkonten zu stehlen, aber auch vielfältige andere Aktionen auszuführen.

Meldungstyp: Command and Control Server

Als Botnet wird eine Menge von kompromittierten Systemen bezeichnet, die sich vollständig unter der Kontrolle eines Angreifers befinden. Dies sind oft normale Arbeitsplatzrechner, in die über eine beliebige Schwachstelle eingebrochen wurde. Nach dem Einbruch installierte der Angreifer eine Bot-Software, die versteckt auf dem System läuft und über einen Control Channel eine Verbindung zu einem zentralen Botnet Control Server hält. Über diesen Botnet Control Server kann der Angreifer dem System, zusammen mit allen anderen von ihm kontrollierten Rechnern, Befehle geben. In der Praxis wird von den Angreifern oft ein IRC- oder HTTP-Server als Command and Control Server verwendet. Die Bot-Software verbindet sich zu diesem und erhält auf diese Weise ihre Befehle.

Wenn Sie eine Meldung bzgl. eines Botnet Control Servers bekommen, wird mit der Hilfe eines Ihrer Systeme ein Botnet gesteuert. Evtl. wird ein regulär von Ihnen betriebener Server für derartige Zwecke missbraucht oder auf einem kompromittierten System wird ein solcher Server betrieben. Sie sollten das betreffende System auf jeden Fall daraufhin untersuchen, ob dort ein nicht autorisierter HTTP- oder IRC-Server läuft. Diese warten häufig auf einem hohen TCP-Port auf eingehende Verbindungen und es ist evtl. eine Vielzahl eingehender oder bestehender Verbindungen zu beobachten.

Teilweise kann bei so einer Meldung lediglich der Zeitpunkt angegeben werden, zu dem der Botnet Control Server zuletzt gesehen wurde.

Im Folgenden sehen Sie ein typisches Beispiel:

```
C&C
---

Textteil:

IP-Adresse:   192.0.2.192
Meldungstyp:  C&C
Zeitstempel:  2014-09-03 14:13:00+02:00
Anzahl:       1
Beschreibung: Das System scheint als Bot-Netz Control-Server missbraucht
              zu werden.

Zuletzt gesehen            IP-Protokoll   Quellport    Zielport  Malware
------------------------------------------------------------------------
---
2014-09-03 14:13:00+02:00  TCP                6668             IRC-Botnet

XML-Anhang:

<message category="C&C" ip="192.0.2.192">
    <description>Das System scheint als Bot-Netz Control-Server missbraucht
zu
werden.</description>
    <event timestamp="2014-09-03 14:13:00+02:00" ip_protocol="TCP"
source_port="6668" cert_diagnosis="IRC-Botnet"/>
</message>
```

Meldungstyp: Configuration

Mit dieser Meldungskategorie versehen wir potentiell unerwünschte Konfiguration von Systemen. Vereinfachen diese auch teilweise die Arbeit mit den Systemen, sind sie doch auch dazu geeignet Angreifern die Arbeit zu erleichtern oder ermöglichen bestimmte Angriffe erst.

Configuration/Open proxy

Ein Proxy fungiert als Stellvertreter für einen Client und führt für diesen Netzwerkanfragen durch. Verbreitet sind z. B. HTTP-Proxies, die Anfragen von Webbrowsern erhalten. Ist die Anfrage nicht aus einem lokalen Cache zu beantworten, wird der zuständige Webserver befragt. Unter einem offenen Proxy wird ein Proxy verstanden, dessen Zugriff nicht eingeschränkt ist und somit auch von Angreifern verwendet werden kann.

Eventuell ist der Proxy Teil einer Bot-Software oder es handelt sich um einen regulären Proxy, der nicht ausreichend gegen Missbrauch abgesichert ist.

Im Gegensatz zu einem Mailserver hinterlässt ein offener Proxy keine "Received"-Zeile im Header der verschickten Mail. Die Konsequenz ist, dass die Spur nur bis zu dem Proxy zurückverfolgt werden kann. D.h. nur die IP-Adresse des Proxies ist im Header der Mail als Quelle zu erkennen. Die IP-Adresse des Angreifers dagegen bleibt verborgen. Potentiell können Proxies für die unterschiedlichsten Protokolle zum Verschicken von Spam missbraucht werden. Beispielweise bietet das HTTP-Protokoll die Möglichkeit, HTTP-Server auf einem beliebigen Port anzusprechen. Dadurch können auch über einen HTTP-Proxy E-Mails verschickt werden. Weiterhin gibt es Standards für Proxies, die unabhängig vom Protokoll das Weiterleiten von TCP- und UDP-Verbindungen ermöglichen, z.B. SOCKS v4 und v5.

Configuration/Open resolver

Ein DNS Resolver ist eine Software, die für die Kommunikation mit einem Nameserver zur Adressauflösung zuständig ist.

Offene Resolver zeichnen sich dadurch aus, dass ihr Zugriff nicht eingeschränkt ist. Folglich können beliebige Systeme im Internet den Resolver verwenden. In Kombination mit gefälschten Absenderadressen in den gestellten Anfragen lassen sich diese somit leicht als Reflektoren für DoS-Angriffe missbrauchen.

Im Folgenden sehen Sie ein typisches Beispiel:

```
Configuration/Open resolver
---------------------------
Textteil:

IP-Adresse:   192.0.2.3
Meldungstyp:  Configuration/Open resolver
Zeitstempel:  2014-09-03 14:15:00+02:00
Anzahl:       1
Beschreibung: Auf dem System scheint ein offener DNS-Resolver betrieben zu
              werden, der potentiell für reflektierte DoS-Angriffe genutzt
              werden kann.

Zuletzt gesehen
-------------------------
2014-09-03 14:15:00+02:00


XML-Anhang:

<message category="Configuration/Open resolver" ip="192.0.2.3">
    <description>Auf dem System scheint ein offener DNS-Resolver betrieben
zu
werden, der potentiell für reflektierte DoS-Angriffe genutzt werden
kann.</description>
    <event timestamp="2014-09-03 14:15:00+02:00"/>
</message>
```

Configuration/Amplifier

Auf dem System scheint ein Dienst betrieben zu werden, der potentiell für reflektierte DoS-Angriffe genutzt werden kann. Das heißt dieser Dienst antwortet auf Anfragen mit gefälschter Absenderadresse und schickt dabei Antworten die ein vielfaches der Größe der Anfrage haben.

Configuration/Unencrypted Communication

Ein von diesem System angebotener Dienst kommuniziert über nicht verschlüsselte Kanäle. Dies ermöglicht es Angreifern abhängig von ihrer Position im Netzwerk, sensitive Daten abzufangen oder zu manipulieren und dadurch falsche Informationen darzustellen.

Configuration/Unrestricted access

Der Zugriff auf einen von diesem System angebotenen Dienst wird anscheinend nicht oder nicht wirksam beschränkt. Abhängig vom Dienst können Angreifer dieses ausnutzen, um auf vertrauliche Informationen zuzugreifen oder Zugang zu diesem oder weiteren Systemen zu erhalten.

Solche Systeme sind beispielsweise offen aus dem Internet erreichbare und nicht ausreichend durch eine Authentifizierung geschützte Industrie-Steuerungssysteme bzw. Systeme zur Gebäudeautomatisierung sowie verschiedene Server-Instanzen (Elasticsearch, Telnet-Server, CouchDB, PostgreSQL-Server).

Meldungstyp: Hosting

Mit dieser Meldungskategorie versehen wir Meldungen über Inhalte, die von einem Angreifer auf Servern Unbeteiligter hinterlegt werden. Diese dienen dazu um z. B. schädliche Inhalte für angegriffene Systeme zum Abruf vorzuhalten.

Hosting/Malware

Angreifer hinterlegen Schadsoftware (sog. Malware) oft auf fremden Systemen mit guter Netzanbindung. Eine Meldung bzgl. Malware auf einem Ihrer Server sehen Sie im Folgenden.

```
Hosting/Malware
---------------

Textteil:

IP-Adresse:   192.0.2.35
Meldungstyp:  Hosting/Malware
Zeitstempel:  2014-09-03 14:16:00+02:00
Anzahl:       1
Beschreibung: Auf dem System wurde Schadsoftware (Malware) zum Download
              bereitgestellt. Die Schadsoftware besteht evtl. aus
              JavaScript Code oder anderen aktiven Web-Inhalten, die auch
              ausgeführt werden, wenn Sie die Seite besuchen. Unter
              Umständen wird sogar versucht Schwachstellen im Browser ohne
              aktive Inhalte auszunutzen. Die Inhalte unter der
              angegebenen URL sollten daher mit größter Vorsicht
              untersucht werden und nicht einfach mit dem eigenen
              Webbrowser. Zum Schutz vor versehentlichen Klicks wurde
              "http" als "hXXp" geschrieben.

Zuletzt gesehen            URL                                  Malware
------------------------------------------------------------------------
2014-09-03 14:16:00+02:00  hXXp://www.example.de/malware


XML-Anhang:

<message category="Hosting/Malware" ip="192.0.2.35">
    <description>Auf dem System wurde Schadsoftware (Malware) zum Download
bereitgestellt. Die Schadsoftware besteht evtl. aus JavaScript Code oder
anderen aktiven Web-Inhalten, die auch ausgeführt werden, wenn Sie die
Seite
besuchen. Unter Umständen wird sogar versucht Schwachstellen im Browser
ohne
aktive Inhalte auszunutzen. Die Inhalte unter der angegebenen URL sollten
daher
mit größter Vorsicht untersucht werden und nicht einfach mit dem eigenen
Webbrowser. Zum Schutz vor versehentlichen Klicks wurde "http" als "hXXp"
geschrieben.</description>
    <event timestamp="2014-09-03 14:16:00+02:00"
source_url="http://www.example.de/malware"/>
</message>
```

Die Schadsoftware war zumindest zu dem angegebenen Zeitpunkt unter der URL erreichbar. Hierbei kann eine ausführbare Datei (.exe wie im obigen Beispiel) oder auch ein Archiv (.rar, .zip) oder ähnliches referenziert werden, das die Schadsoftware enthält.

Weiterhin ist es möglich, dass Webseiten angegeben werden. Dabei handelt es sich in der Regel um manipulierte Seiten, die versuchen, Schwachstellen im Webbrowser des Benutzers auszunutzen. Dies erfolgt oft nicht direkt auf der angegebenen Seite, sondern teilweise nach mehrfacher Umleitung mit Hilfe von nicht sichtbaren Iframes.

Sollten Sie eine Meldung zu einer Webseite erhalten, ist auf jeden Fall Vorsicht geboten, da auch Ihr Webbrowser möglicherweise anfällig ist. Die Iframes werden außerdem in der Regel nicht vom Webbrowser dargestellt, so dass eine Manipulation leicht übersehen werden kann.

Aufgrund von falschen Klassifikationen durch Virenscanner kann es bei diesem Meldungstyp vereinzelt zu Falschmeldungen kommen.

Hosting/Phishing

Angreifer imitieren mit sog. Phishing Sites die Webseiten von Banken oder bekannten Internet-Diensten (z. B. eBay, Amazon). Deren Kunden werden durch Spam-Mails auf die Phishing Site gelockt, damit diese sich dort vermeintlich anmelden. Tatsächlich werden die von den Nutzern eingegebenen Informationen an die Angreifer weitergeleitet und zum Teil sofort für Betrug oder Diebstahl verwendet.

Einem Phishing Angriff geht oft eine Kompromittierung des Webservers durch einen SSH Account Probe oder eine verwundbare Web-Anwendung voraus. Wenn Sie eine Meldung bzgl. einer Phishing Site erhalten, wird Ihr Webserver aktiv für Betrug verwendet und die Phishing Seite sollte umgehend offline genommen werden. Eine typische Meldung finden Sie hier.

Weitere Informationen zu dem Thema sind u. a. auf https://apwg.org/ zu finden.

Meldungstyp: Scan

Mit dieser Meldungskategorie versehen wir Aktivitäten von Systemen, die in den Bereich Aufklärung fallen. Angreifer suchen vor dem eigentlichen Angriff häufig Netzbereiche nach potentiell verwundbaren Systemen ab. Dabei versuchen sie zu ermitteln, ob ein System einen bestimmten Dienst anbietet oder eine bestimmte, verwundbare Version einer Software ausführt. Der eigentliche Angriff auf diese als verwundbar identifizierten Systeme erfolgt dann in einem zweiten Schritt.

Scan/Portscan

Bei einem Portscan versuchen Angreifer herauszufinden, auf welchen Systemen ein bestimmter Dienst angeboten wird oder es wird versucht, alle angebotenen Dienste eines Systems zu erkunden. Da Portscans häufig an einer Firewall entdeckt werden, ist oftmals nicht klar, ob dem Portscan direkt ein Angriff gefolgt wäre oder ob es beim Portscan geblieben wäre. Portscans werden häufig über kompromittierte Systeme ausgeführt, deshalb sollten Portscans trotz ihrer Häufigkeit nicht ignoriert werden. Im Folgenden sehen Sie ein typisches Beispiel.

```
Scan/Portscan
-------------

Textteil:

IP-Adresse:   192.0.2.34
Meldungstyp:  Scan/Portscan
Zeitstempel:  2014-09-03 14:21:00+02:00
Anzahl:       2
Beschreibung: Das System fiel durch wiederholte Verbindungsversuche auf
              (Portscans). Evtl. ist das System kompromittiert und es wird
              nun nach weiteren verwundbaren Systemen gesucht.

Zuletzt gesehen            IP-Protokoll   Quellport    Zielport  Malware
------------------------------------------------------------------------
---
2014-09-03 14:18:00+02:00  ICMP                                  Nachi
2014-09-03 14:21:00+02:00  UDP               41521       30247


XML-Anhang:

<message category="Scan/Portscan" ip="192.0.2.34">
    <description>Das System fiel durch wiederholte Verbindungsversuche auf
```

```
(Portscans). Evtl. ist das System kompromittiert und es wird nun nach
weiteren
verwundbaren Systemen gesucht.</description>
    <event timestamp="2014-09-03 14:18:00+02:00" ip_protocol="ICMP"
cert_diagnosis="Nachi"/>
    <event timestamp="2014-09-03 14:21:00+02:00" ip_protocol="UDP"
source_port="41521" target_port="30247"/>
</message>
```

Für Portscans muss keine vollständige TCP-Verbindung aufgebaut werden, wodurch sich Möglichkeiten für Falschmeldungen ergeben:

- "Chaffing": Hierbei versucht der Scanner seine IP-Adresse dadurch zu verschleiern, dass gleichzeitig noch weitere Pakete mit gefälschten Adressen an das Ziel gesendet werden, so dass nur eine der verschiedenen Quelladressen tatsächlich dem Angreifer zuzuordnen ist.
- Windows Messenger Popup Spam: Dieses wird an die UDP-Ports 1026 bis 1029 gesendet. Ziel ist es dabei, eine Nachricht an den Windows Messenger-Dienst zu senden, um beim Nutzer eine Textbox zu öffnen. Da der Port TCP/135 meistens durch eine Firewall gesperrt ist, weichen die Angreifer auf die altenativen UDP-Ports aus, auf denen der Dienst ebenfalls zu erreichen ist.
- Backscatter: Tritt bei Denial of Service Angriffen auf, bei denen z.B. ein Webserver mit einer Vielzahl von SYN-Paketen an einen offenen TCP-Port überlastet wird. Da der Angreifer hier nicht an einer Antwort interessiert ist, kann der Absender beliebig gefälscht werden. In diesem Fall antwortet das angegriffene System mit einem ACK-Paket an die gefälschte Absenderadresse (sog. Backscatter). Wurden IP-Adressen Ihres Netzwerkes als Absender missbraucht, werden die Antworten vermeintlich als Portscan interpretiert. Backscatter kann zum größten Teil anhand der Ports und der gesetzten TCP-Flags erkannt werden.

Meldungstyp: SPAM

Wenn Sie eine derartige Meldung erhalten, wurde von einem Ihrer Systeme unerwünschte Werbemail (SPAM) verschickt. Dies kann durch eine Schadsoftware oder eine Bot-Software geschehen sein. Möglich sind auch reguläre Proxy-Server, die nicht ausreichend gegen Missbrauch gesichert sind oder Webserver, auf denen eine verwundbare Web-Anwendung betrieben wird. Im Folgenden sehen Sie ein typisches Beispiel.

```
Spam
----

Textteil:

IP-Adresse:   192.0.2.1
Meldungstyp:  Spam
Zeitstempel:  2014-09-03 14:22:00+02:00
Anzahl:       1
Beschreibung: Das System ist durch das Verschicken von unerwünschter
              Werbemail (sog. SPAM) aufgefallen.

 Zuletzt gesehen             Quellport    Zielport
-------------------------------------------------
2014-09-03 14:22:00+02:00       22777          25


XML-Anhang:
```

```
<message category="Spam" ip="192.0.2.1">
    <description>Das System ist durch das Verschicken von unerwünschter
Werbemail (sog. SPAM) aufgefallen.</description>
    <event timestamp="2014-09-03 14:22:00+02:00" source_port="22777"
target_port="25"/>
</message>
```

Wenn wie in diesem Fall nur ein Zeitpunkt vorliegt, nicht jedoch die eigentliche Werbemail, sind Falschmeldungen möglich. Liegen Informationen vor, dass das System auch auf der Composite Blocking List wegen Versand von Werbemail aufgenommen wurde, wird eine entsprechende URL angegeben.

Meldungstyp: Vulnerability

Mit dieser Meldungskategorie informieren wir über Systeme, die nicht ausreichend gegen aktiv ausgenutzte Schwachstellen abgesichert sind.

Vulnerability/CVE-2019-0708

Auf dem System wird ein Windows-RDP-Dienst betrieben, der nicht ausreichend gegen die unter dem Namen 'Bluekeep' bekannte Schwachstelle CVE-2019-0708 abgesichert ist. Die Schwachstelle wird bereits aktiv von Angreifern ausgenutzt, um betroffene Systeme vollständig zu kompromittieren.

Weitere Informationen finden Sie im DFN.Security-Portal:

https://portal.security.dfn.de/advisories/details/2019-0977

Vulnerability/CVE-2019-19781

Das System ist ein Citrix Gateway (früher NetScaler Gateway) und nicht ausreichend gegen CVE-2019-19781 gesichert. Die Schwachstelle wird seit Januar 2020 aktiv ausgenutzt. Es ist davon auszugehen, dass das System mittlerweile kompromittiert ist und neu aufgesetzt werden muss.

Weitere Informationen hierzu finden Sie unter:

https://support.citrix.com/article/CTX267027

und im DFN.Security-Portal:

https://portal.security.dfn.de/advisories/details/2019-2658

Vulnerability/CVE-2021-44228

Auf dem System wird das Logging-Werkzeug Log4j in einer Version eingesetzt, die nicht ausreichend gegen die unter dem Namen "Log4Shell" bekannte Schwachstelle CVE-2021-44228 abgesichert ist. Die Quelle der Daten ist, soweit bekannt, angegeben.

Weitere Informationen hierzu finden Sie unter:

https://www.dfn-cert.de/aktuell/log4j-kritische-schwachstelle-CVE-2021-44228.html

Vulnerability/Exchange-Server

Diese Meldung weist auf den Einsatz eines Microsoft Exchange Server hin, der durch kritische Schwachstellen (CVE-2021-26855, CVE-2021-34473, CVE-2021-26427, CVE-2021-42321) verwundbar ist, für die Sicherheitsupdates bereitstehen.

Vulnerability/FortiGate VPN

Das System ist ein FortiGate SSL VPN und nicht ausreichend gegen aktuelle Schwachstellen abgesichert. Die Schwachstellen werden bereits aktiv von Angreifern ausgenutzt, um VPN-Server vollständig zu kompromittieren.

Weitere Informationen hierzu finden Sie unter:

https://fortiguard.com/psirt/FG-IR-18-383

https://fortiguard.com/psirt/FG-IR-18-384

https://fortiguard.com/psirt/FG-IR-18-388

https://fortiguard.com/psirt/FG-IR-18-389

und im DFN.Security-Portal:

https://portal.security.dfn.de/advisories/details/2019-2658

Vulnerability/Pulse Connect VPN

Das System ist ein Pulse Connect Secure Server und nicht ausreichend gegen CVE-2019-11510 und CVE-2019-11539 abgesichert. Die Schwachstellen werden bereits aktiv von Angreifern ausgenutzt, um VPN-Server vollständig zu kompromittieren.