Bayerisches Landesamt für Verfassungsschutz

Cyber-Allianz-Zentrum Bayern

Bayerisches Landesamt für Verfassungsschutz · Postfach 45 01 45 · 80901 München

Ihre Zeichen, Ihre Nachricht vom	Unser Zeichen		München
	337-S-060000.1/194/5		27.07.2015
Bearbeiter/in	**E-Mail**	**Telefon**	**Telefax**
Hr. Dr. Stelte	caz@lfv.bayern.de	089 31201-222	

Warnmeldung - Modus Operandi chinesischer APT-Gruppen

Sehr geehrte Damen und Herren,

die deutschen Sicherheitsbehörden, wie auch internationale IT-Dienstleister, analysieren GOTHIC PANDA als eine von vielen aktiven Tätergruppen. Die IT-Dienstleister benennen die Angreifer leider recht unterschiedlich. Die Gruppierung wird vom IT-Dienstleister Mandiant als APT-3, von FireEye als Clandestine Fox oder Clandestine Wolf und von Crowdstrike als GOTHIC PANDA bezeichnet. Das Cyber-Allianz-Zentrum Bayern im Bayerischen Landesamt für Verfassungsschutz konnte Indikatoren über die genutzte Infrastruktur der Angreifer ermitteln. Die APT-Gruppen GOTHIC PANDA und DESTORY PANDA (APT-18) nutzen beide aktuell die Schwachstelle CVE-2015-5119 für Spearphishing Angriffe auf Unternehmen und staatliche Stellen. In diesem Bericht wird der Modus Operandi bekannter und mutmaßlich chinesischer APT-Gruppen beschrieben.

Die mutmaßlich chinesischen Angreifer der APT-Gruppe GOTHIC PANDA nutzen für Angriffe auf Unternehmen häufig zuvor übernommene Server zur Verschleierung des Angriffsweges. In einer ersten Phase werden für die Angreifer leicht zu übernehmende Server angegriffen und übernommen. In einer zweiten Phase nutzen die Angreifer diese Server für den Angriff auf ihr eigentliches Ziel. Für den Angriff werden Spearphishing-Emails vorbereitet und an die Opfer verschickt. In den Emails wird ein Link auf die von den Angreifern kontrollierten Webserver angeboten. Bei dem Besuch der Webseite wird die Schwachstelle **CVE-2015-5119** ausgenutzt, um Schadprogramme (wie etwa PlugX, Pirpi, etc.) auf den Client des Opfers einzuschleusen.

Neben den beiden APT-Gruppen GOTHIC PANDA und DESTORY PANDA ist auch die APT-Gruppe HURRICANE PANDA bekannt. Während GOTHIC PANDA für elektronische Angriffe gekaperte Infrastruktur nutzt, verwendet DESTORY PANDA zumeist angemietete Infrastruktur. DESTORY PANDA unterscheidet sich von den anderen Gruppen in der Art wie die eige-

ne Infrastruktur (C2-Server) angesprochen wird; man verwendet meistens keine DNS-Auflösung – C2-Server werden direkt mit der IP-Adresse angesprochen. Jedoch sind auch DNS-Domänennamen nicht in jedem Fall ein sicherer Indikator. Varianten des Trojaners PlugX nutzen das DNS Protokoll für die Kommunikation mit den Steuerungs-Servern (C2-Server).

```
Frame 6620: 154 bytes on wire (1232 bits), 154 bytes captured
(1232 bits)
Ethernet II, Src: Cisco_xx (00:24:14:xx:xx:xx), Dst: Netscreen_xx
(00:10:db:xx:xx:xx)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 994
Internet Protocol Version 4, Src: 185.25.49.64, Dst: x.x.x.x
User Datagram Protocol, Src Port: domain (53), Dst Port: 60996
(60996)
Domain Name System (response)
    Request In: 6616
    Time: 0.043981000 seconds
    Transaction ID: 0x8ee4
    Flags: 0x8480 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries

EODDCIPBGIBADEKOAAAAAAAAAAAAAAAAAAAAAAAA.addert.plkis7s2.com:
type TXT, class IN
            Name:
EODDCIPBGIBADEKOAAAAAAAAAAAAAAAAAAAAAAAA.addert.plkis7s2.com
            Type: TXT (Text strings)
            Class: IN (0x0001)
    Answers

EODDCIPBGIBADEKOAAAAAAAAAAAAAAAAAAAAAAAA.addert.plkis7s2.com:
type TXT, class IN
            Name:
EODDCIPBGIBADEKOAAAAAAAAAAAAAAAAAAAAAAAA.addert.plkis7s2.com
            Type: TXT (Text strings)
            Class: IN (0x0001)
            Time to live: 3 seconds
            Data length: 18
            Text: AAAAAABCGIBADEKO
            Text:
```

Abbildung 1: Kommunikation über das DNS Protokoll (DNS-Tunnel / PlugX)

Die APT-Gruppe HURRICANE PANDA nutzt für die DNS-Auflösung eigene DNS-Nameserver (angemietet z. B. bei HURRICANE ELECTRIC) und verschickt übliche DNS-Anfragen zu Domains, wie etwa *github.com* oder *pinterest.com*, an diese Nameserver. Die Antwort des Nameservers ist dann eine IP-Adresse eines Rechners der Angreifer und nicht die zu erwartende korrekte IP-Adresse.

Erste Phase: Aufbau der Infrastruktur des Angriffs

Die Angreifer suchen sich für den eigentlichen Angriff Server aus, die mutmaßlich für den Betreiber nicht kritisch sind und daher nicht prioritär beobachtete werden. Gerade im universitären Umfeld, aber auch bei kleineren Unternehmen sind solche Server häufig anzutreffen.

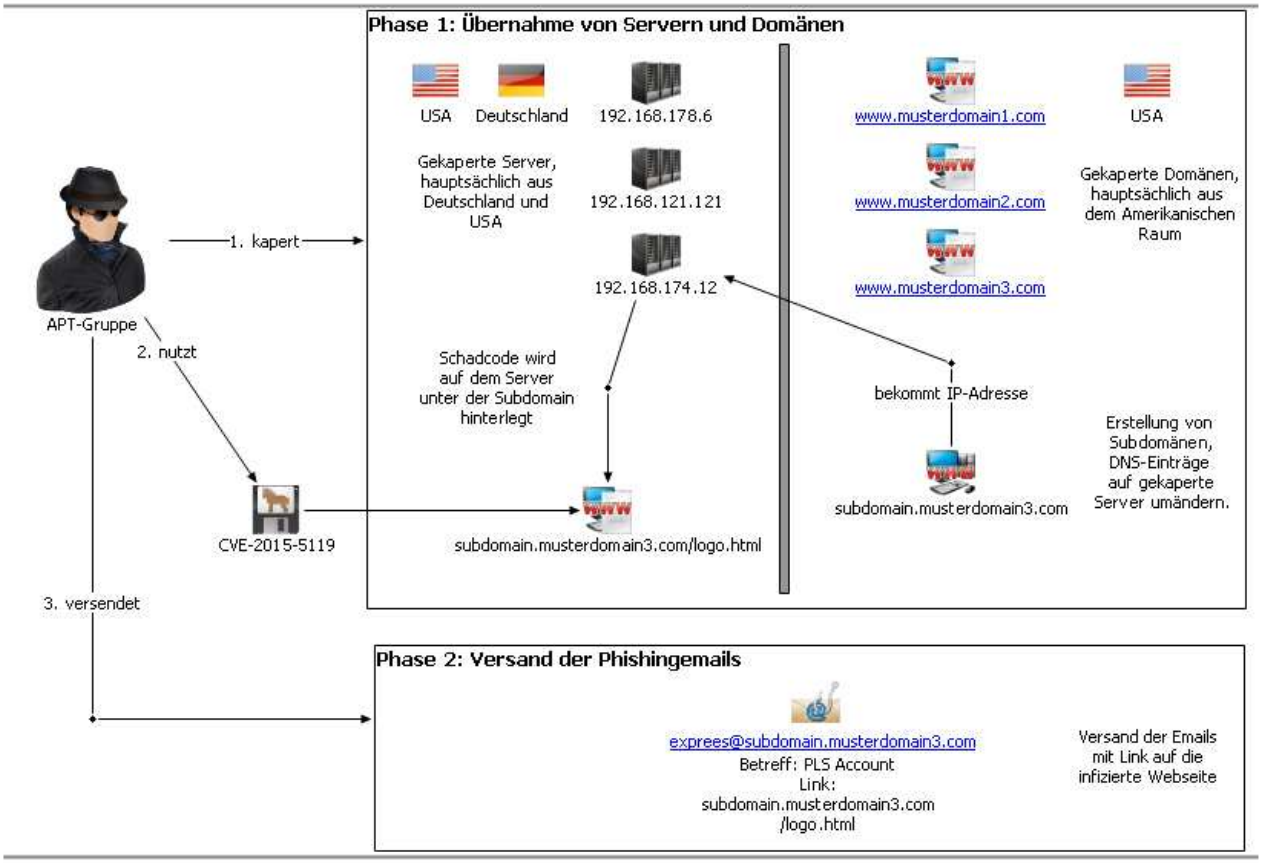

Abbildung 2: Modus Operandi GOTHIC PANDA - Aufbau der Infrastruktur zur Infektion der Ziele

Ein Beispiel für die Übernahme eines solchen Servers kann wie folgt aussehen. Ein Rechner eines kleineren Unternehmens wird als Internet-Gateway für externe Mitarbeiter gelegentlich genutzt. Den Administratoren des Rechners ist bereits von einigen Wochen aufgefallen, dass der Internet-Datenverkehr merklich langsamer wurde. Zunächst schien sich der Protokollierungsdienst syslogd aufgehängt zu haben. Durch eine spätere nähere Untersuchung konnte festgestellt werden, dass in den Protokolldaten des Paketmanagers Aktivitäten festgehalten wurden, die nicht von der Administration stammen. Am 18.6.2015 wurde der Webserver-Dienst nginx installiert und am 30.6.2015 wieder deinstalliert. Bei der Deinstallation wurden alle Konfigurations-, Protokolldateien und die über die vom Webserver-Dienst angebotenen Dateien entfernt. In System-Protokolldateien konnten zudem SSH Zugriffe festgestellt werden. Benutzt wird hierbei das Public-Key Verfahren des SSH-Dienstes. Da die Administrato-

ren auf diesen Server keinen SSH Public-Key eingetragen haben, muss es den Angreifern gelungen sein, diesen einzutragen und für einen administrativen Fernzugriff zu nutzen.

Befehl-Historie:

/var/log/apt/history.log
Start-Date: 2015-06-18 16:42:13
Commandline: apt-get install -y nginx

Start-Date: 2015-06-30 03:25:07
Commandline: apt-get purge nginx

Verwendeter SSH Public-Key der Angreifer (/root/.ssh/authorized_keys):

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFY1I0MsVFW5jvLbTriLQZCxT2dh/ohzEt9kfaCRlIa
ExHGt/NAviAmkiIDGAYQUAAxRTmcPB4PTi9vsCOwtLxd8KhAwA8cbg/Agl0BrgQTYEtJ6VdcD
Q8UHsFV0vmPbcrfOAOw9gb16AiQP62PuTevCCkOoVxhwfLB7B7noll61qU4rwYVD1an2NIWRo
c+dzCepKZ6h6pJspQ/be4G+vET1Hdru9ZoFCA+AZ9Na5RzjVKoMxdE1tmNVaO0wjpW3nNgCAX
6joWjWdqDrW/dVCY5utSL807AmSU/9eiwncYYy8+BLf2BE0byB/HQ5YhInh2/5lAnvPjYY4SX
RJNfq21 root@localhost

Die Angreifer haben für Fernadministration die nachfolgenden IP-Adressen verwendet.

IP:	Geolocation:	Anbieter:	Hinweis:
61.63.74.209	Taiwan	Kbtelecom.net, Taiwan	verm. gekapert
74.208.97.115	USA	1and1.com, USA	Keine Domänen
114.38.73.66	Taiwan	Hinet.net, Taiwan	Keine Domänen
114.38.64.98	Taiwan	Hinet.net, Taiwan	Keine Domänen

Der IP-Adressblock 74.43.2.0/24 ist nach Auffassung des BayLfV vermutlich ebenfalls den Angreifern zuzuordnen.

Zweite Phase: Spearphishing Angriff unter Ausnutzung der zuvor übernommen Infrastruktur

Über das Versanddatum der Emails an Angriffsziele konnten die zuständigen Nameserver für die jeweilige Domäne gesucht werden. Hierbei wurde festgestellt, dass der Domäne ein MX Eintrag für die Zeit des Spearphishing-Angriffs mit einer entsprechenden MX-Priorisierung unter Verwendung einer plausiblen Subdomäne (z. B. mail3.xxx.xxx.) hinzugefügt wurde. Die Angreifer müssen somit Zugriff auf die Domänenverwaltung gehabt haben. Durch den Eintrag des MX-Records sind bekannte SPAM-Abwehrmaßnahmen, wie etwa Helo-Check und DNS-Reverse-Check, wirkungslos.

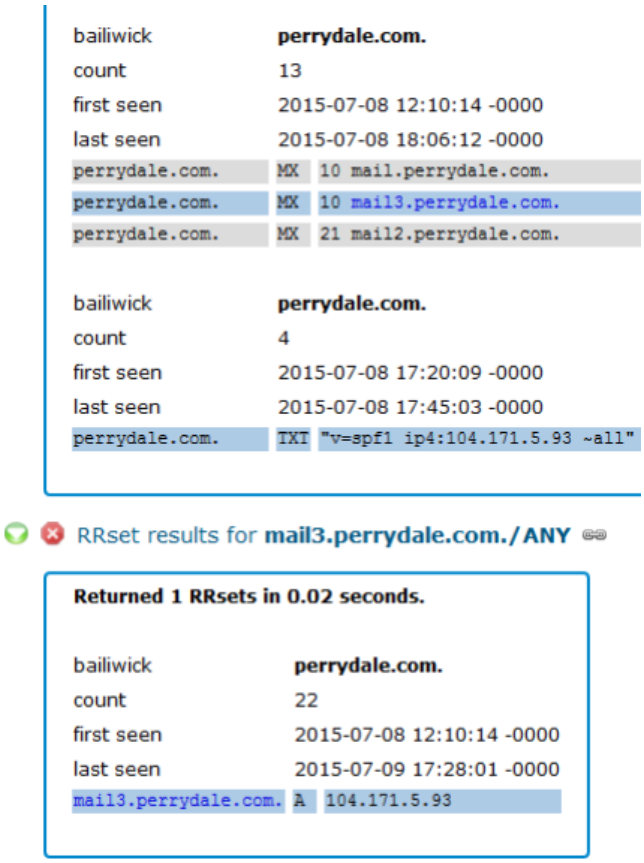

Abbildung 2: MX-Record eingefügt für die Zeit der EMail-Kommunikation (Quelle: DNSDB)

Die nachfolgenden IP-Adressen sind als genutzte Infrastruktur für Spearphishing Angriffe (Dateiablage für den Exploit) bekannt.

IP:	Provider:	Land:	Domäne:
95.143.41.5	Inline, Deutschland	Deutschland	fr.skybolt.com
148.251.176.87	Hetzner, Deutschland	Deutschland	was.solidimageinc.com
5.231.68.214	Ghostnet, Deutschland	Deutschland	it.racsa.com
62.108.40.241	Comsitec, Deutschland	Deutschland	item.solidimageinc.com
85.214.149.123	Strato, Deutschland	Deutschland	iam.amirart.com
218.161.78.26	Data Communication, TW	Taiwan	i18n.linux.org.tw
193.110.75.118	OJSC Promtelecom, UA	Ukraine	uiamp.org.ua; en.r-u.org.ua; ml.*
107.161.179.15	HostDime.com, USA	USA	Pay.alyusrsms.com
198.23.153.190	Colocrossing, USA	USA	gti.tarimex.com

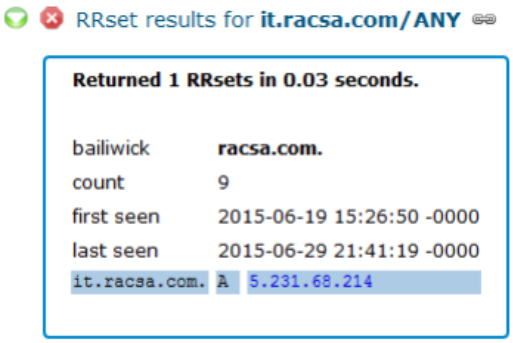

Abbildung 3: Eintrag einer Subdomäne (Quelle: DNSDB)

Spearphishing Angriffe müssen nach offenen Informationen amerikanischer Quellen im Zeitraum 6 bis 9. Juni 2015 stattgefunden haben. Die Webseiten der übernommenen Server waren jedoch bis spätestens 30. Juni 2015 aktiv. Es ist zu vermuten, dass Spearphishing Angriffe in mehreren Wellen im Juni stattgefunden haben.

Beispielsweise werden die nachfolgenden Links in der Email angeboten:

http://uiamp.org.ua/wp-read/[alphanumerische Zeichen].html
http://pay.alyusrsms.com/uuid/[alphanumerische Zeichen].html
http://en.r-u.org.ua/en/[alphanumerische Zeichen].html
http://ml.r-u.org.ua/message/[alphanumerische Zeichen].html
http://item.solidimageinc.com/alerts/[alphanumerische Zeichen].html
http://fr.skybolt.com/express/[alphanumerische Zeichen].html
http://item.solidimageinc.com/alerts/[alphanumerische Zeichen].html
http://it.racsa.com/it/[alphanumerische Zeichen].html
http://item.solidimageinc.com/pro/[alphanumerische Zeichen].html
http://rpt.perrydale.com/en/show.swf
http://report.perrydale.com/ema/show.swf
http://rpt.perrydale.com/en/b.gif
http://report.perrydale.com/ema/b.gif
http://rpt.perrydale.com/en/rep201507101.pdf

Als Betreffzeile sind die nachfolgenden Bezeichnungen bislang bekannt:

Up to $200 off for You
Order Status Changed
PLS Account
AEP Energy Program Update: 2015 Program Year Kick Off
Happy Father's Day!
D71311884 (n°de transport)
Happy Father's Day!
EM6155944(n°de transport)
SII SecureMail Identity Verification - Do Not Reply

BBW Analysis report- 2015
Tomorrow Morning New Starts
Perrydale Club for Leadership: Financial Literacy 101
FAS Analysis report-2015
Review Link
$200-450 off refurbished imacs
Free Shipping on iPad Mini
How can I change my account security information?
Increases your IQ by 130 points
The NEW! MacBook starting at $1,299!
No. [alphanumerische Zeichen]
PLS Account [alphanumerische Zeichen]
USDOT Access PIN

Die Gruppen nutzen zur Ausschleusung von Dateien und zur Ausbreitung im Rechnernetz bspw. Schadprogramme der Trojaner-Familie PlugX oder auch bekannte Programme, wie etwa Mimikatz und psexec. Weitere bekannte Schadsoftware wird von den Gruppen in unterschiedlicher Häufigkeit verwendet. Hierzu zählen die Trojaner Pirpi, SOGU, Sakula und Gh0stRat, wie auch der China Chopper Webshell und ScanBox Exploit.

Als Rückkanalwege der nachgeladenen und genutzten Schadprogramme oder Email-Versender sind die folgenden Indikatoren bekannt:

107.20.255.57
125.227.139.53
23.99.20.198
27.255.83.46
194.44.130.179
125.227.139.53
137.175.4.132
198.55.115.71
210.109.99.64
192.184.60.229
104.151.248.173
101.55.27.3
amxil.opmuert.org
bwxt.com
dublincore.org
ivc.jiscs.com
link.angellroofing.com
psa.perrydale.com
rpt.perrydale.com
report.perrydale.com
tech.hotelicon.net
gs2.playdr2.tw
gs3.playdr2.tw
gs4.playdr2.tw
km-nyc.com
km153.com

Im Verdacht ein Rückkanalweg für eine verwendete Schadsoftware zu sein, sind die nachfolgenden Indikatoren:

199.93.37.19	http	http://199.93.37.19/send/[alphanumerische Zeichen]/
84.53.175.45	http	http://84.53.175.45/send/[alphanumerische Zeichen]/
8.12.207.19	http	http://8.12.207.19/send/[alphanumerische Zeichen]/
ns71.domaincontrol.com	DNS-Tunnel	[alphanumerische Zeichen].NDAJDOGDJIMNP
ns72.domaincontrol.com	DNS-Tunnel	[alphanumerische Zeichen].NDAJDOGDJIMNP
185.25.49.64	DNS-Tunnel	[alphanumerische Zeichen].addert.plkis7s2.com
185.25.49.64	DNS-Tunnel	[alphanumerische Zeichen].addert.plkis7s2.com

Weiterführende Informationen zu der Schadsoftware PlugX finden Sie auf den nachfolgenden Webseiten:
https://www.fireeye.com/blog/threat-research/2014/07/pacific-ring-of-fire-plugx-kaba.html
http://labs.lastline.com/an-analysis-of-plugx-using-process-dumps-from-high-resolution-malware-analysis
https://www.circl.lu/pub/tr-24/
http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-malware-found-in-official-release-of-league-of-legends-path-to-exile/

Weiterführende Informationen zu den APT-Gruppen finden Sie auf den nachfolgenden Webseiten:

http://info.publicintelligence.net/FBI-GovernmentSpearphishing.pdf
http://www.threatconnect.com/news/the-anthem-hack-all-roads-lead-to-china/
http://blog.crowdstrike.com/storm-chasing
https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf
https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html
https://www.fireeye.com/blog/threat-research/2015/07/second_adobe_flashz.html
https://www.fireeye.com/blog/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
http://community.websense.com/blogs/securitylabs/archive/2015/04/24/opportunity-knows-no-boundary-a-case-study-of-acquisition.aspx
https://www.threatstream.com/blog/scanbox-waterhole-kit
http://blog.dynamoo.com/2015/07/evil-network-malicious-rats-including.html

Trotz sorgfältiger Prüfung der Signaturliste können sich Fehler einschleichen. Wenn Ihnen eine fehlerhafte Zuordnung auffällt, bitten wir um eine Rückmeldung ihrerseits.

Mit diesem Schreiben übermitteln wir Ihnen im Anhang Signaturen zu den beschriebenen APT-Gruppen. Die Signaturen sollen Sie bei der Erkennung und Abwehr von Cyberangriffen unterstützen. Bitte beachten Sie, dass die Signaturen auch zu False-Positive Meldungen führen können.

Diese vertraulichen Informationen sind ausschließlich zur firmeninternen Verwendung. Eine Weitergabe an Dritte ist erst nach vorheriger Rücksprache mit dem Cyber-Allianz-Zentrum Bayern möglich. Eine Weitergabe an ein von Ihnen mit der Administration Ihres Rechnernetzes betrauten Unternehmen ist erlaubt.

Mit freundlichen Grüßen

gez. Schinabeck
Leitender Regierungsdirektor