Botnetzangriffe mit Honeypots analysieren

Klebefallen

Markus Manzke

Seit etwa zwei Jahren sind Honeypots – Buzzword: Deception Technologies – als ernst zu nehmender Bestandteil im Sicherheitsportfolio der Unternehmens-IT im Kommen. Ein Blick auf die Ursachen dafür und neue Ansätze beim Einsatz dieses Verfahrens.

In den Frühzeiten des kommerziellen Internets erlebten Honeypots einen ersten Hype (siehe Onlinequellen sowie „Alle Links“, [a–d]), schafften es aber nicht zur Marktreife und blieben in der akademischen Nische. In einem Talk auf der BlackHat 2015 erläuterten die Macher von Thinkst die Historie von Honeypots und warum diese in der Vergangenheit ein Mauerblümchendasein gefristet haben [e].

Mittlerweile erweisen sich Honeypots als hilfreich im Arsenal der Verteidiger und erfreuen sich einer Gartner-Studie zufolge wachsender Beliebtheit [f]. Einerseits können diese Tools Eindringlinge im Frühstadium des Angriffs auffliegen lassen und beschäftigen. Andererseits liefern sie gute Daten zur Bedrohungslage von Rechenzentren, die Onlinedienste anbieten und Anomalien frühzeitig erkennen müssen.

Die Ausgangslage in Sachen IT-Sicherheit ist denkbar schlecht: Während das eigene Netzwerk schon aus wirtschaftlichen Gründen nie absolut sicher sein kann, hat ein Angreifer die Wahl der Waffen. Er kann in Ruhe nach Schwachstellen suchen und Art und Zeitpunkt des Angriffs bestimmen. Soziale Netzwerke erleichtern das Social Engineering heutzutage enorm, das immer noch einen großen Anteil am Erfolg oder Misserfolg eines gezielten Angriffs (Spear Phishing) hat, wie die Attacken auf den Bundestag, RSA, Google, Apple und andere populärer Einbrüche der letzten Jahre zeigen. Traditionelle Sicherheitsvorkehrungen wie das Installieren von Firewalls oder Virenscannern versagen bei sogenannten „Advanced Persistent Threats“ [g] und maßgeschneiderten Einmal-Exploits oder Drive-by-Downloads, da die Erkennung von Malware zumeist signaturbasiert erfolgt und Unbekanntes nicht erkannt wird. Einen weiteren Angriffspunkt bieten Smartphones und Tablets (BYOD), die schwieriger durch die Sicherheitsinfrastruktur eines Unternehmens geschützt werden können als Server, PCs und Notebooks.

Mit Honeypots fängt man Eindringlinge

Unter diesen Voraussetzungen steht zu befürchten, dass die erste Phase eines gezielten Cyberangriffs auf eine Organisation – nämlich das Einrichten eines dauerhaften Zugangs zum Netz – in vielen Fällen erfolgreich sein wird und das vorherrschende Prinzip der „Eggshell Security“ dies nicht verhindern kann. Verizons „Data Breach Investigation Report 2014“ nennt knapp 1400 Vorfälle, in denen Angreifer erfolgreich in Netze eingedrungen sind und Daten aus dem Unternehmen entwenden konnten [h]. Über 90 % dieser Angriffe kamen von außen, also über das Internet.

Wenn ein Angreifer die äußere Hülle erst einmal geknackt hat, steht ihm mehr als genug Zeit zur Verfügung, das interne Netz zu erkunden, die interessanten Daten zu finden und aus dem Netzwerk auszuleiten. Mandiant spricht von mehr als 200 Tagen, die Angreifer durchschnittlich für Zugriffe auf erfolgreich angegriffene Ziele nutzen können [i].

Diese Lücke sollen Honeypots schließen. Sie können erfolgreiche Angriffe in der zweiten Phase entdecken und melden, also sobald der Angreifer anfängt, seinen Brückenkopf ins Netzwerk auszubauen, die weitere interne Infrastruktur aufzuklären und lohnende Ziele zu identifizieren. Honeypots erkennen Angreifer allein aufgrund ihres Verhaltens, benötigen also keine Signaturen. In einem Netz mit 100 Servern können sich beispielsweise 30

Honeypots verstecken, die Angreifer auf den ersten Blick nicht von anderen Systemen unterscheiden können, weil sie auf das jeweilige Netz abgestimmt und ohne nähere Untersuchung nicht als Fallen erkennbar sind.

Honeypots können heute fast alle Systeme bis zu einem gewissen Grad simulieren: Fileserver, Webserver, Mailserver, Switches, Proxies, Datenbankserver, Application-Server, SCADA-Systeme (Supervisory Control and Data Acquisition – messen, steuern, regeln), Workstations, Firewalls und so weiter.

Derlei Systeme sitzen an unterschiedlichen Stellen im Netzwerk und warten darauf, dass jemand auf sie zugreift. Sollte ein Angreifer von außen oder innen auf der Erkundungstour den jeweiligen Sensor scannen oder näher untersuchen, geht ein Alarm an eine Auswerteeinheit, die ein SIEM (Security Information and Event Management) oder andere Monitoring-Systeme benachrichtigt. Als Reaktion darauf können verschiedene Maßnahmen folgen. So lassen sich alle Verbindungen nach außen und innen trennen, die auf den Angreifer zurückzuführen sind, und das entsprechende Personal wird alarmiert.

Honeypots sollen nicht nur einen Einbruch in einer möglichst frühen Phase melden, also bevor der Angreifer tiefer ins Netz vorgedrungen ist, damit der Angegriffene geeignete Gegenmaßnahmen einleiten kann. Sie binden auch Ressourcen des Angreifers und erhöhen dessen Aufwand, da er mehr Systeme untersuchen muss. Überdies tragen sie wertvolle forensische Daten zur späteren Analyse und Verfolgung zusammen.

So weit die Theorie. Praktisch gibt es keine Klick-and-run-Sicherheitslösungen. Das gilt besonders für Honeypots. Während man in kleineren Netzen einige wenige Honeypots schnell zum Laufen bekommt, ist der Aufwand in größeren, segmentierten Netzen mit vielen Servern wesentlich höher, da nur eine sorgfältige Planung und Integration in die IT der Organisation einen ausreichenden Nutzen verspricht.

Wenn jemand eine neue Schwachstelle publiziert (hier einen Bittorrent-DDoS), registrieren Honeypots kurz darauf ein rasch wachsendes Interesse der Scanner (Abb. 1).

Honeypots ergänzen jedenfalls eine Defense-in-Depth-Strategie, da sie erfolgreiche Angreifer aufspüren, bevor die sich weiter im Netz festsetzen können, und sie kommen für Organisationen infrage, die besonders schützenswerte Daten vorhalten und mit gezielten Angriffen rechnen müssen: Neben Unternehmen gehören dazu Behörden, Regierungs- und Forschungseinrichtungen sowie größere Versorgungseinrichtungen und Infrastrukturanbieter.

Externe Bedrohungen erkennen

Nicht nur im internen Netz sammeln Honeypots wertvolle Daten. Im Internet platzierte Exemplare geben Aufschluss über die Bedrohungslage für Onlinedienste und Server. Heutzutage ist irgendwie alles „Cloud“ und jeder dank der allgegenwärtigen Smartphones ständig online. Die Apps nutzen häufig Webtechnologien, und komplette Cloud-Server lassen sich für wenige Euro pro Monat mieten. Leistungsfähige Systeme wie NoSQL-Datenbanken (ElasticSearch, MongoDB, Redis) lassen sich schnell in Betrieb nehmen. Die Kehrseite der Medaille: Solche Systeme bilden die Grundlage für serverbasierte Botnetze, da sie aufgrund angreifbarer Default-Konfigurationen und anderer Sicherheitslücken unerlaubte Zugriffe gestatten.

Neue Verfahren im Bereich netzwerkweiter Scans (ZMap, MASSCAN) ermöglichen es, das gesamte IPv4-Internet innerhalb weniger Stunden nach verwundbaren Systemen abzusuchen. Mit Shodan steht eine Suchmaschine zur Verfügung [j], die zum Beispiel mehr als 8000 ElasticSearch-Installationen weltweit findet, deren Großteil über eine RCE-Lücke angreifbar ist.

Weltweit verteilte Sensoren, die angreifbare Dienste und Applikationen simulieren, sammeln laufend Daten über die Bedrohungslage durch diese Bots. Eine Karte stellt Statistiken dieser Angriffe tagesaktuell dar [k]. Eine solche Infrastruktur kann zum Aufklären von vielerlei Angriffen beitragen. Neben Brute-Force-Login-Versuchen (Mail, SSH, Datenbanken, RDP, Webapplikationen) sind Exploits von Diensten wie MongoDB, ElasticSearch oder Redis zu sehen, aber auch Exploits älterer JBoss-/Tomcat-Versionen oder populärer Open-Source-Webanwendungen.

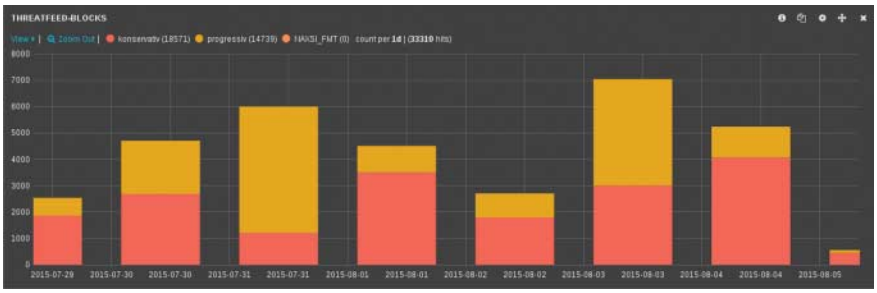
Wahlloses Ausprobieren aller Exploits

Automatisierte Angriffe finden oft auf recht wahllose Weise statt. Wenn ein Webserver auf Port 80 lauscht, probieren Angreifer praktisch jeden Exploit der letzten Jahre durch: ShellShock, PHPMyAdmin, Joomla, JBoss, diverse WordPress-Exploits, PHP (*cgi-bin*), TimThumb-Lücke und viele weitere – unabhängig davon, ob die entsprechenden Applikationen oder Programmiersprachen überhaupt verfügbar sind. Das Ziel der meisten Exploits ist es, Server per Remote Code Execution (RCE) in Botnetze zu integrieren und Ressourcen für das Versenden von Spam, weitere Exploit-Scans oder DDoS-Angriffe zu missbrauchen.

Das Blog „Malware Must Die!“ hält ausführliche Analysen zu allen Arten von Linux-Server-Malware vor [l], angefangen von PHP-/Perl-Bots bis hin zu Binaries, die auf den jeweiligen Prozessortyp abgestimmt installiert werden und durch Kompilieren die Command-and-Control-Server verschleiern sollen. Details einer serverseitigen Botnet-Infektion mit Einblicken in die Methoden der „Botmaster“ finden sich zudem unter [m]. Wie gefähr-

iX-TRACT

- Honeypots – scheinbar angreifbare, tatsächlich aber protokollierende Systeme – können dazu beitragen, Einbrüche in Netze und Hosts rechtzeitig zu erkennen.
- Täter, die sich mit Honeypots auseinandersetzen, stehen weniger Ressourcen für wirksame und schädliche Angriffe zur Verfügung.
- Honeypot-Systeme sammeln wertvolle Daten zur späteren Analyse der Vorgänge und zur Verfolgung der Angreifer.



Durch den Einsatz von IP-Reputationseinschätzungen lassen sich viele Angriffe von vornherein unterbinden (hier pro Tag und IP-Adresse, Abb. 2).

Zwei Phasen eines DDoS-Angriffs auf je einen Provider in der Ukraine und in Russland im Juni 2015 (Abb. 3)

lich RCE-Lücken in Webapplikationen sind, belegt eine Analyse aus dem Frühjahr 2013: Ein WordPress-Botnet mit 90 000 Servern kann offenbar ganze Providernetze lahmlegen [r]. Wer ein serverbasiertes Honeynet betreibt, kommt rasch zu der Überzeugung: Wer ungepatchte Applikationen oder verwundbare Dienste betreibt, muss sich nicht fragen, ob, sondern wann die Kompromittierung erfolgt.

Nach Erfahrung des Autors dauert es nach dem Publizieren einer Schwachstelle nur ein bis zwei Tage, bis die ersten Scanner danach suchen. Nach spätestens vier Wochen sind die automatisierten Skripte der Angreifer so weit angepasst, dass ab dann mit einem Exploit zu rechnen ist. Eine kleine Artikelserie erläutert dieses Verhalten beispielhaft [n, o]:

– Eine Sicherheitslücke wird veröffentlicht.
– Am selben Tag gehen einige Honeypots mit angreifbaren Softwareversionen online.

Das Dashboard eines Honeypot-Netzwerks gibt Live-Einblicke in die Aktivität eines DDoS-Botnetzes (Abb. 4).

– Nach knapp 30 Stunden zeigt sich ein signifikanter Anstieg der Scans von durchschnittlich drei auf mehr als 100 Zugriffe pro Tag.
– Nach drei Wochen sind die automatisierten Scanner so weit angepasst, dass täglich etwa 7000 Zugriffe auf die Honeypots stattfinden.

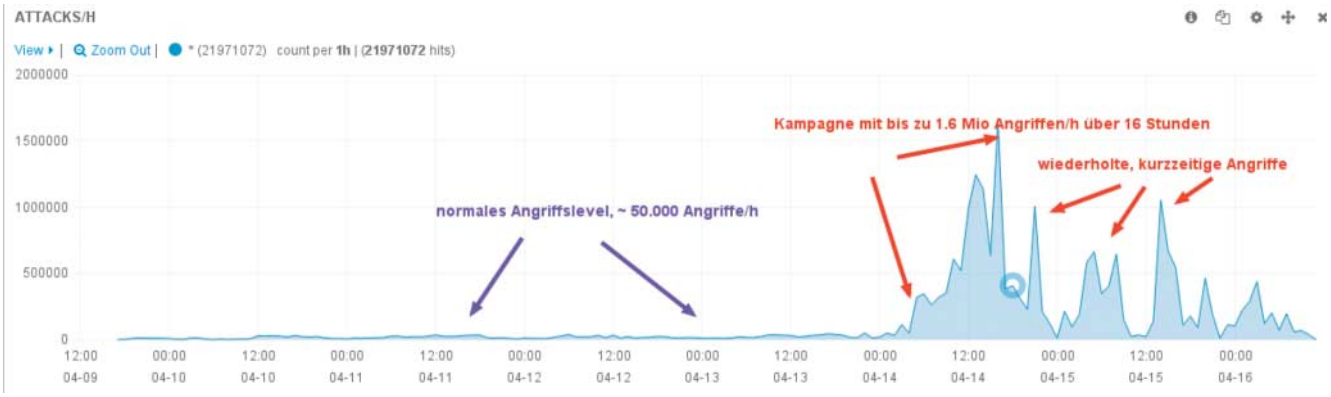
Globale, serverbasierte Honeynets dienen häufig dem Monitoring von IP-Adressen und deren Reputationseinschätzung. Dadurch, dass ein Honeynet rund um die Uhr Informationen über automatisierte Angriffe sammelt, lassen sich Angreifer anhand der von ihnen genutzten IP-Adressen erkennen und blockieren. Sinnvoll ist dies für Online-Rechenzentren, die populäre Open-Source-Software hosten (WordPress, TYPO3, Magento, XTCommerce etc.) und die häufig von Sicherheitslücken betroffen sind [p]. Aber auch Cloud-(Server)-Anbieter können eine Adressreputation etwa dafür einsetzen, Massen-Exploits gegen Tools wie ElasticSearch und MongoDB einzudämmen.

Honeynets liefern darüber hinaus Ansatzpunkte zum Einschätzen der Risiken für industrielle SCADA-Systeme, die gar nicht mit dem Einsatzzweck „Internet“ entwickelt wurden, mittlerweile aber daran angeschlossen sind. Der TÜV Süd hat beispielhaft ein Honeynet in Form eines simulierten Wasserwerks betrieben und analysiert, welche Zugriffe und Angriffe auf ein solches System im Laufe mehrerer Monate stattfinden [q]. Honeynets können massive Exploit-Kampagnen aufdecken [s]. Viele treten um Weihnachten und Ostern herum auf oder sobald jemand eine neue, lohnenswerte Lücke publiziert.

Botnetzangriffe analysieren

Sogenannte Low-Interaction-Honeypots (LIH) zum Detektieren von Angriffsversuchen lassen sich recht einfach installieren und betreiben [w]. Ein LIH emuliert einen angreifbaren Dienst, ohne aber den kompletten Funktionsumfang bereitzustellen. Zum Einrichten eines LIH reicht es, einen entsprechenden Port zu öffen und jede Anfrage mit ein paar Zufallsdaten zu beantworten. LIHs dienen insbesondere der Gewinnung statistischer Daten und lassen sich von menschlichen Angreifern rasch identifizieren. Zum Aufzeichnen der Zugriffe automatisierter Scanner und Angriffsskripte reichen sie aber allemal.

Eine Herausforderung besteht dagegen in High-Interaction-Honeypots, die sich infizieren und in Botnetze integrieren lassen, um diese zu analysieren und Infor-



Analyse eines Angriffs auf einen chinesischen Provider im April 2015 auf der Basis von Honeypot-Daten (Abb. 5)

mationen über die angegriffenen Ziele zu liefern [t, u, v]. Es sind meist vollständige Server, die „angreifbare" Dienste bereitstellen. Sie sind schwieriger einzurichten und zu verwalten als LIH. Der Fokus bei einem High-Interaction-Honeypot liegt nicht auf automatisierten Angriffen, sondern darauf, manuell ausgeführte Angriffe zu beobachten und zu protokollieren, um so neue Methoden der Angreifer rechtzeitig zu erkennen.

Wenn es sich um Botnetze auf Basis eines Internet Relay Chat (IRC) handelt, lassen sich diese von innen aufklären und alle im Botnet befindlichen Server identifizieren. Eine kleine Unvorsichtigkeit kann jedoch schnell zu einer unangenehmen Antwort des Botmasters führen. Falls er erkennen sollte, dass sein Botnet infiltriert wurde, könnte er etwa per DDoS-Angriff antworten – und das wäre eine vergleichsweise harmlose Reaktion. Als Belohnung für dieses Risiko warten Einsichten in Funktionsweise und Angriffsverhalten eines DDoS-Botnetzes.

Das Team des Autors konnte zum Beispiel heftige Angriffe auf russische und ukrainische Rechenzentren beobachten [x]. Mit über 100 GBit/s wurden mehrere Tage lang zwei Provider lahmgelegt. Eine spätere Analyse ergab, dass das Botnet aus über 10 000 Bots bestand und dass die Botmaster über fortschrittliche Tools verfügen mussten, um bei dieser relativ kleinen Anzahl an Bots einen konstanten Datenstrom aufrechterhalten zu können. Auffällig bei diesem Angriff war zudem, dass die Angreifer sämtliche IP-Adressen

der RZ angriffen, sogar solche, die gar nicht konnektiert waren.

Dadurch war ein Null-Routing nicht möglich und das RZ war komplett offline.

Entweder wollten die Angreifer das eigentliche Ziel verschleiern oder so viel Schaden wie möglich anrichten. Der Angriff selbst dauerte neun Tage und bestand aus zehn Wellen. Jede davon bestand aus einer 30- bis 60-minütigen Einschwingphase und dem eigentlichen Angriff, der jeweils zwischen 6 und 14 Stunden dauerte. Während der Einschwingphase testeten die Täter wahrscheinlich die Kapazität des Botnetzes, um dann den Angriff mit konstanter Intensität stundenlang ausführen zu können.

Ein weiterer Trend, der sich durch „Honeybots" beobachten lässt, sind DDoS-Angriffe mithilfe sogenannter „Booter" oder „Stresser" auf DSL-Leitungen [y]. Da diese mit höherer Frequenz während der Ferienzeiten stattfinden und parallel dazu vermehrt Gaming-Server angegriffen werden, könnte es sich um gelangweilte Jugendliche handeln, die sich gegenseitig per DDoS-Angriff aus dem Netz schießen. Auswahl gibt es genug: Schon für 15 US-$ per Kreditkarte gibts einen Account bei einem Booter-Service, mit dem man DSL-Anschlüsse und schwachbrüstige Server leicht lahmlegen kann. DDoS as a Service hat Konjunktur, und neben einem Großteil der Dienste, die mit 20 bis 100 MBit/s feuern können, gibt es einige teurere Services, die bis zu 5 GBit/s liefern.

Ein weiteres Ergebnis der Honeybots: Durchschnittlich sind 30 bis 50 Prozent der Angriffe erfolgreich und der angegriffene Host nicht mehr erreichbar. Damit sind DDoS-Angriffe aus wirtschaftlicher Sicht ernst zu nehmende Bedrohungen. Ein Teil der Daten, die die „blinden Passagiere" liefern, ist online in einem Live-Dashboard verfügbar [z].

Fazit

Honeypot-Infrastrukturen können interne und externe Bedrohungen analysieren und transparent machen. Sie helfen Betreibern von Onlinediensten, sich gegen automatisierte Angriffe zu schützen, und können im internen Netz potenzielle Eindringlinge aufspüren, bevor sie sich festsetzen.

Auch im Bereich der Reputationsbewertung sind Honeynets wertvolle Werkzeuge zum Erkennen von Botnetzen im eigenen Netz, etwa bei Internetprovidern und Hosting-Anbietern. Und ganz nebenbei eignen sich Honeynets wunderbar zum Analysieren serverbasierter Botnetze. (un)

Markus Manzke

arbeitet als Experte für IT-Security bei der 8ack GmbH in Kiel.

Onlinequellen

[a] The Government of the Hong Kong Special Administrative Region; Honeypot Security
www.infosec.gov.hk/english/technical/files/honeypots.pdf

[b] Symantec; The Value of Honeypots, Part One: Definitions and Values of Honeypots
www.symantec.com/connect/articles/value-honeypots-part-one-definitions-and-values-honeypots

[c] WindowSecurity.com; Honeypots – Definitions and Value of Honeypots
www.windowsecurity.com/whitepapers/honeypots/Honeypots_Definitions_and_Value_of_Honeypots.html

[d] SANS; Honeypots: A Security Manager's Guide to Honeypots
www.sans.edu/research/security-laboratory/article/honeypots-guide

[e] Thinkst Thoughts; BlackHat 2015 – Bring Back the HoneyPots
http://blog.thinkst.com/2015/08/blackhat-2015-bring-back-honeypots.html

[f] Gartner; Emerging Technology Analysis: Deception Techniques and Technologies
https://www.gartner.com/doc/3096017/emerging-technology-analysis-deception-techniques

[g] Advanced Persistent Threat
https://de.wikipedia.org/wiki/Advanced_Persistent_Threat

[h] Verizon; 2014 Data Breach Investigation Report
www.verizonenterprise.com/de/DBIR/2014/

[i] Mandiant; 2014 Threat Report
https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

[j] Suchmaschine „Shodan" für beliebige ans Internet angeschlossene Geräte (hier: Suche nach „elasticsearch")
https://www.shodan.io/search?query=elasticsearch

[k] Global Attack Map
http://8map.de/maps/

[l] Malware Must Die!
http://blog.malwaremustdie.org/

[m] ElasticZombie – Inside an ElasticSearch-Botnet
https://8ack.de/analysen/elastic_zombie_inside_an_elasticsearch_botnet

[n] Swell on the Horizon – Watching Scanners Searching for Bittorrent Clients
https://8ack.de/analysen/swell_on_horizon-bittorrent_ddos_scans

[o] Sets Arriving – Watching Scanners Searching for Bittorrent Clients
https://8ack.de/analysen/sets_arriving-bittorrent_ddos_scans

[p] Exploit Database (hier: Suche nach „WordPress")
https://www.exploit-db.com/search/?action=search&description=wordpress

[q] Potenzielle Angreifer sind überall
www.tuev-sued.de/tuev-sued-konzern/presse/pressearchiv/potenzielle-angreifer-sind-ueberall

[r] Brute Force Attacks Build WordPress Botnet
http://krebsonsecurity.com/2013/04/brute-force-attacks-build-wordpress-botnet/comment-page-1/

[s] Server-Botnetz mit massiven SSH-Brute-Force-Attacken
https://8ack.de/analysen/ssh_botnet_brute_force_attack_de

[t] How to Catch a Hacker in the Act
http://motherboard.vice.com/read/how-to-catch-a-hacker-in-the-act

[u] SSH Brute Force – The 10 Year Old Attack That Still Persists
https://blog.sucuri.net/2013/07/ssh-brute-force-the-10-year-old-attack-that-still-persists.html

[v] High-Interaction Server Honeypots
https://de.wikipedia.org/wiki/Honeypot#High-Interaction_Server_Honeypots

[w] Low-Interaction Server Honeypots
https://de.wikipedia.org/wiki/Honeypot#Low-Interaction_Server_Honeypots

[x] DDoS-Angriffe auf ukrainische und russische Rechenzentren
https://8ack.de/analysen/ddos_angriffe_auf_ukrainische_rechenzentren

[y] DDoS for Hire: Six Nabbed for Using LizardSquad Attack Tool
http://krebsonsecurity.com/category/ddos-for-hire/

[z] BotPit – DDoS Attack Dashboard
http://8map.de/dashboard

Alle Links: www.ix.de/ix1512098