PLXsert INTERNAL THREAT ADVISORY

PROLEXIC
DDoS Attacks End Here.

Critical BOTNET and Operation Profile

CONFIDENTIAL

GSI ID: 1066

Risk Factor - High

OVERVIEW

DAY 1: January 28, 2014

At 15:50 UTC (10:50 a.m. EST) on Tuesday, January 28, Prolexic detected a distributed denial of service (DDoS) attack against a major financial institution. The attack traversed Prolexic's global DDoS mitigation infrastructure, ending approximately six hours later, at 19:56 UTC (4:56 p.m. EST).

Three financial institutions reported being targets of an identical DDoS framework. At 8:59 a.m. EST, a group calling itself the European Cyber Army (ECA) claimed responsibility for the attacks.

Figure 1: ECA announced the attack via Twitter Tuesday morning

The first ECA tweets warning of a possible disruption of service started around 8 a.m. EST, coinciding with the opening of U.S. banking operations. At about the same time, other individuals began posting tweets mentioning the instability of their online banking services.

The attack escalated throughout the day, peaking at 18:48 UTC (1:48 p.m. EST) with 190 Gbps of attack bandwidth and 97 Mpps of attack volume. This set a record for attack bandwidth mitigated by Prolexic.

CAMPAIGN ATTRIBUTES

The following attributes were observed:

- **Attack type:** SYN flood, UDP flood, DNS flood
- **Source port:** Randomized
- **Target port:** 80,443,53
- Sample payloads are shown in Figure 2

```
IP X.X.X.X.59359 > X.X.X.X.80: Flags [S], seq 1845917519, win 5840,
options [mss 1460,sackOK,TS val 957417280 ecr 0,nop,wscale 7], length 0

IP X.X.X.X.58428 > X.X.X.X.443: Flags [S], seq 649980021, win 14600,
options [mss 1460,sackOK,TS val 3383825736 ecr 0,nop,wscale 7], length 0

IP X.X.X.X.59117 > X.X.X.X.53: Flags [S], seq 1627597156, win 14600,
options [mss 1460,sackOK,TS val 151951039 ecr 0,nop,wscale 8], length 0

IP X.X.X.X.78 -> X.X.X.X DNS 1457 Unknown operation (11) 0x5e5e  Unknown
(24158) <Unknown extended label> Unknown (24158) <Unknown extended label>
Unknown (24158) <Unknown extended label> Unknown (24158) <Unknown extended
label> Unknown (24158) <Unknown extended label> Unknown (24158) <Unknown
extended label> Unknown (24158) <Unknown extended label> Unknown (24158)
<Unknown extended label> Unknown (24158) <Unknown extended label> Unknown
(24158) <Unknown extended label> Unknown (24158) <Unknown extended label>
Unknown (24158) <Unknown extended label> Unknown (24158) <Unknown extended
label> Unknown (24158) <Unknown extended label> Unknown (24158) <Unknown
extended label> Unknown (24158) <Unknown extended label> Unknown<snip>

IP X.X.X.X.36599 > X.X.X.X.80: UDP, length 1407
E...~.@.8.E.g..5.......P....5555555555555555555555555555555555555555555
555555555555555555555555555555555555555555555555555555555555555555555555
555555555555555555555555555555555555555555555555555555555555555555555555
555555555555555555555555555555555555555555555555555555555555555555555555
5555555555<snip>

IP X.X.X.X.48358 > X.X.X.X.443: UDP, length 1424
E.....@.8..,g.&2...........qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
qqqqqqqqqqqqq<snip>
```

Figure 2: Sample malicious payloads from incoming attack traffic

SOURCE CLAIMING RESPONSIBILITY

ECA also claimed responsibility for DDoS attacks against other Prolexic customers around 3:43 p.m. EST.

Third-party intelligence received by the Prolexic Security and Engineering Response Team (PLXsert) indicates that one of the tools used in this attack matches the Brobot signature used during the Operation Ababil campaign against American financial institutions in 2013. While Operation Ababil was claimed by Al-Qassam Cyber Fighters (QCF), there seem to be many similarities between the groups.

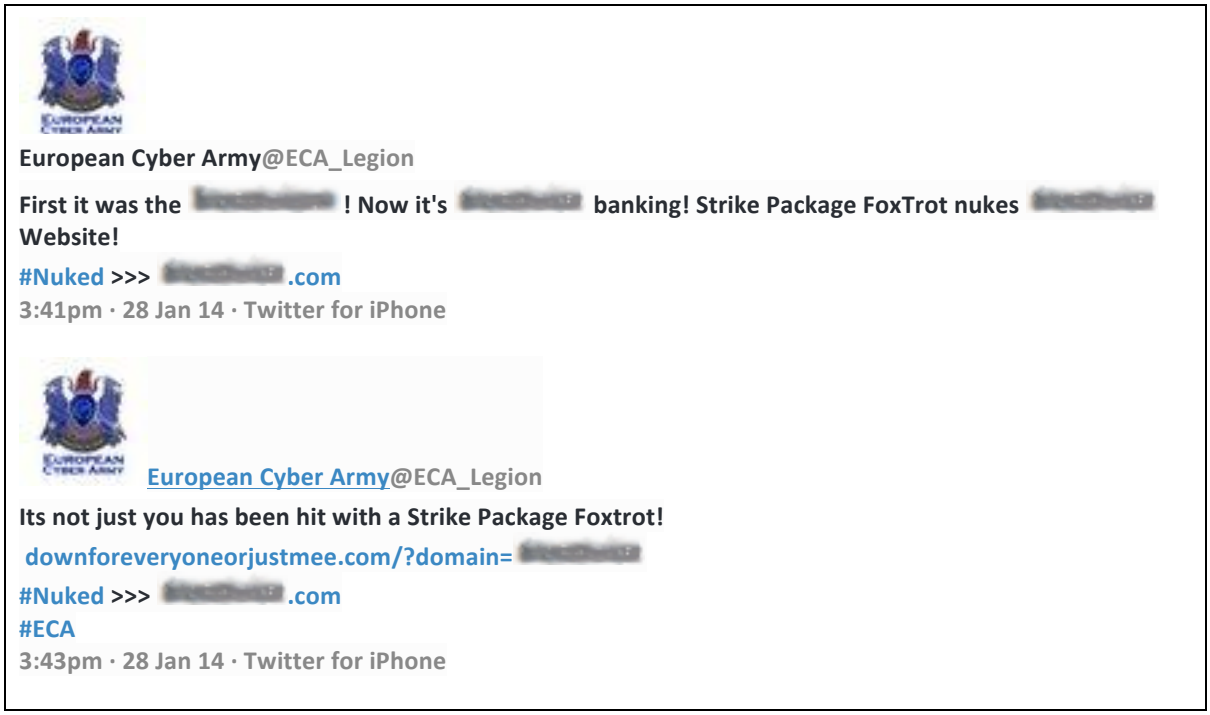

Figure 3: ECA claiming authorship of the attacks (target names redacted)

Both of the targets mentioned in Figure 3 were previously targeted by QCF with the identical toolkit used in the most recent attacks. However, a quick review of the QCF website revealed a lack of updates since October 21, 2013. This coincides with the lull in attacks experienced by US banking institutions.

Figure 4: The QCF blog has not been updated since October 21, 2013

ECA attempted to obfuscate the motives behind the recent DDoS attack campaign by associating themselves with previous hacktivists causes taken up by the Anonymous collective, as shown in the ECA tweet in Figure 5.

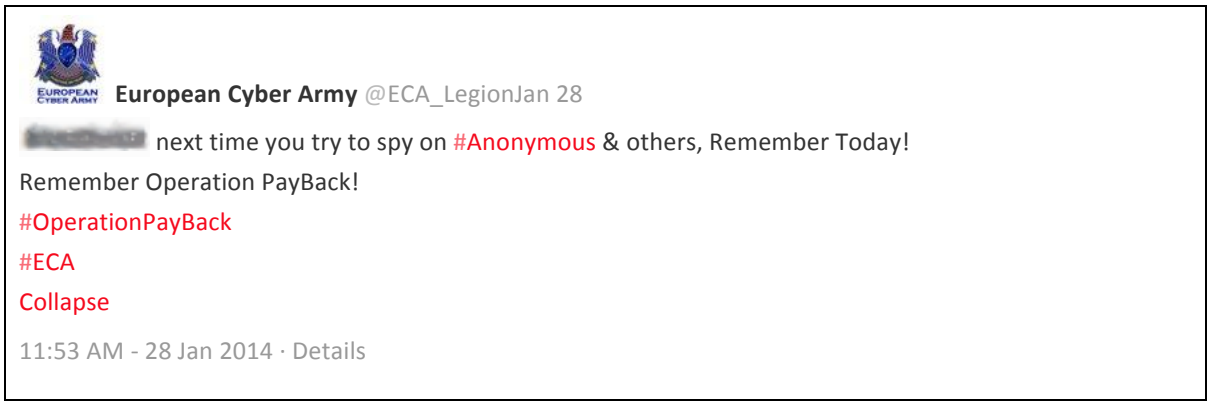

Figure 5: ECA justifying attacks in retaliation for spying on Anonymous

The ECA Twitter handle appears to have multiple users, as indicated by the varying grammar, word choice and spelling styles. The style tends to change after 4 p.m. EST (21:00 London) (24:00 Tehran).

Before the emergence of QCF and Operation Ababil last year, there was at least one known group that orchestrated attack campaigns against major American financial institutions: L0ngWave99. This group claimed to support the Occupy Wall Street movement and performed several attack campaigns before disappearing suddenly. PLXSert has reviewed the code evolution of the tool used in these campaigns. Forensic analysis shows that the tools were used by both groups and also revealed similarities in coding patterns – and probably development by the same authors.

As the U.S. banking day drew to a close, ECA announced additional attacks, as shown in Figure 6.

Figure 6: ECA announcing more upcoming attacks

DAY 2: January 29, 2014

On the second day of the campaign, ECA published bank account numbers, allegedly belonging to WikiLeaks founder Julian Assange for his defense, and subsequently announced DDoS attacks against U.S. military targets, as shown in Figure 7.

Figure 7: ECA announced additional DDoS attack targets

ECA also retweeted a link to a blog post where DDoS toolkit vendors noted similarities to the 2013 QCF attacks. Other users on Twitter seemed to associate ECA behavior with past QCF actors as well.

Figure 8: ECA tweets a media report discussing the campaign

DAY 3: January 30, 2014

ECA and others continued to tweet about the attacks on U.S. targets, as shown in Figure 9.

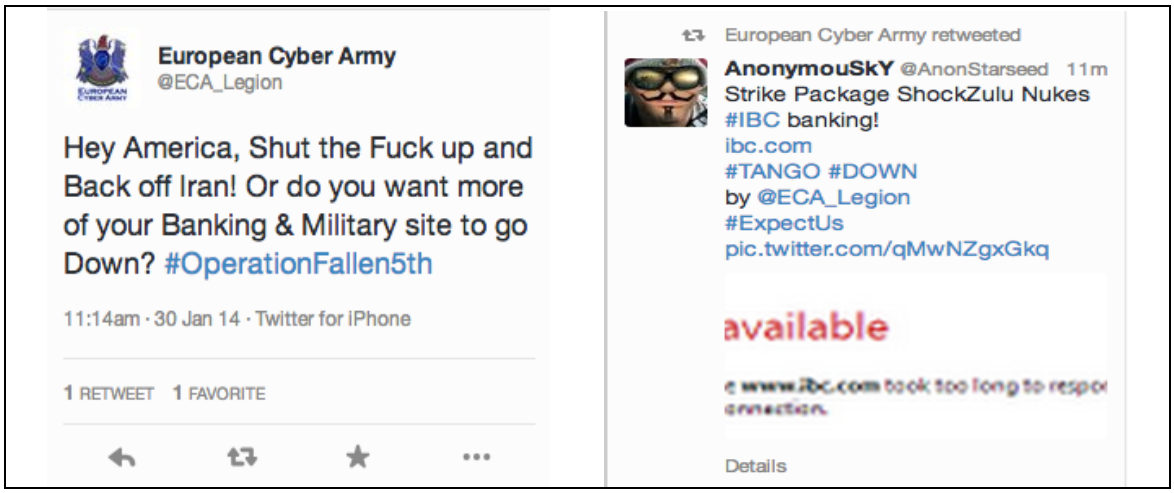

Figure 9: ECA and others continue to publicize the DDoS campaign on day three

INFECTION MODIFICATIONS

PLXSert confirmed the pervasive presence of Kloxo web administration panels on many of the infected bots that participated in these DDoS attacks. Kloxo versions 5.75 and 6.1.6 have several known vulnerabilities and exploits that have been publicized.[1] A trait associated with QCF operations is the use of publicly available exploits to compromise large numbers of web servers. Historically, the group's main targets were WordPress and Joomla installations.

[1] http://www.exploit db.com/search/?action=search&filter_page=1&filter_description=&filter_exploit_text=kloxo&filter_author=&filter_platform=0&filter_type=0&filter_lang_id=0&filter_port=&filter_osvdb=&filter_cve=

Although it is too early to show with certainty that ECA is related to QCF, there are significant indicators that match the modus operandi of QCF. These include:

- Similar attack signatures
- Similar attack hours of operation
- The use of public exploits against large numbers of web servers
- Similar botnet structures
- Similar public personas

PLXSert will continue to process the attack code and research the features of this botnet. Further threat updates will be released as warranted.

CONTRIBUTORS

PLXsert

ABOUT THE PROLEXIC SECURITY ENGINEERING AND RESPONSE TEAM (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post-attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

ABOUT PROLEXIC

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, energy, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Fort Lauderdale, Florida and has scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.