Angler Exploit Kit Featured in Mass Phishing Campaign

Proofpoint security researchers recently detected and analyzed a highly distributed multi-day phishing campaign sent to Proofpoint customers and other organizations. In a classic example of a longline phishing campaign, the overall campaign was comprised of more than 46,000 unique IP addresses and included more than 1.8 million messages. Nearly 80 percent of the IP addresses only sent one message to a receiving organization.

Designed to deliver advanced malware to recipients who clicked on the included link, the phishing email itself is simple and straightforward. It plays on user concerns that they may already be the victim of an account hijacking. The spam email link redirects users to a compromised site that in turn redirects to the Angler exploit kit (EK). Angler is currently integrating exploits for Microsoft Internet Explorer, Microsoft Silverlight, and Adobe Flash. If infected, users would be exposed to a Zeus variant that would give attackers a foothold in the victim's computer and organization.

Moreover, this series of emails is one of the largest exploit-based, malware-delivering campaigns in recent months. The most recent occurrence of an Angler campaign was in March 2014, which attempted to deliver GameOver Zeus and Cutwail. The shift in this broadly-targeted campaign to an unidentified Zeus variant reinforces the effectiveness of the recent GameOver Zeus takeover initiative.

Campaign Timeline and Details

The first wave of the campaign was detected on June 13, when Proofpoint technology detected a series of emails using an account alert template ("Your Online Access has been temporarily disabled"). Nearly 750,000 messages were sent over two hours to a broad recipient base, including 6,000 to a single organization. The domains used by spammers were highly rotated and designed to avoid proactive spam detection. In addition, source IP addresses were highly distributed, with more than 20,000 unique IP addresses each sending a single message to the receiving organization.

Examples are below:

---

**Your Online Access has been temporary disabled**

Customer Support

Sent: Friday, June 13, 2014 at 4:24 AM

To: 

Dear 

Your Online Access has been temporarily disabled. Someone with IP address 42.128.240.236 tried to login into your account from an unrecognized device.

Please click on the link below to restore your online access and confirm your identity. We strongly recommend you to restore your online access within 72 hours after this message was delivered. Otherwise your account will be closed due to the Terms of Use of the Service. Restore your Access.

Mail sent to this address cannot be answered.
Angler Exploit Kit Featured in mass Phishing Campaign

The detected sample delivered a Zeus variant, which had relatively broad detection on VirusTotal, with 18 out of 54 engines detecting it. This is consistent with a mass-custom "longlining" campaign, rather than a more targeted spear phishing attack.

As is typical for this type of campaign, the malicious senders focused on frontloading delivery to the first 15-30 minutes in order to defeat typical anti-spam measures. While no solution can guarantee 100 percent effectiveness against such a large and distributed attack, anti-spam solutions featuring intelligent, predictive rules can ensure that the bulk of the initial wave is blocked.

Notable in this case, the spammers waited approximately 90 minutes and initiated a second wave with a modestly revised template, new URLs, and different sending IP addresses. Through the predictive rules in place on Proofpoint's systems and the updates made in response to the earlier version of the campaign, no messages in the second wave were delivered to our customers.

Four days later, on June 17, a new spam campaign containing links redirecting to the Angler EK targeted several Proofpoint customers. Similar to the campaign detected on June 13, this effort employed three new and improved email templates: one voicemail reminder ("New voicemail received") and two billing reminders ("Help & Advice – British Gas" and "Virgin Media Automated Billing Reminder").

Examples are below:
You have received a Voicemail. Follow the link below to listen to it

[link to listen]

Help & Advice – British Gas
British Gas
Sent: Tuesday, June 17, 2014 at 4:26 AM
To: [redacted]

You can find your invoice for June 2014 by click on link below
[link to invoice]

We may want to contact you by mail, phone, visit or e-mail about other products and services provided by us, or our partners. By providing your information you will be indicating your consent to us keeping you informed in this way but please tick the box if you DO NOT wish to hear about such products and services.

© British Gas 2014

Virgin Media Automated Billing Reminder

Date 17th June 2014

[content of e-mail]

[signature]

[link to e-billing]

Please click on the link to login to e-billing. You will need to login using your primary e-mail address.

Kind Regards,

Virgin Media
Customer Services Team
[company logo]
Proofpoint’s cloud-based solution and big-data analytics enabled our researchers to see the attackers adjust in real time. As attackers reacted to the effectiveness of frontline anti-spam rules, they employed created variants and sent them mid-campaign.

Proofpoint analytics detected an 80 percent overlap of sender IP addresses between the June 17 and June 13 campaigns. Our technology confirmed these addresses used the same botnet and exploit kit. There is a strong likelihood that both campaigns were initiated from the same malicious party.

There are several important benefits and takeaways from this detection and analysis:

- The tens of thousands of unique sending IP addresses involved in the campaign exemplify the complexity of today’s email-based threats, and the inability of traditional signature- and blacklist-based defenses to stop them.
- Attackers are continually monitoring and adjusting their campaigns in real time to evade updates to existing defenses. Only intelligent, predictive defenses can anticipate changes, adjust detection and modify blocking to stop new email and malware variants.
- Identifying these campaigns and determining that they are related is a vital insight that enables security solution providers, such as Proofpoint, to better hone our systems for future detection. It helps organizations better respond to these campaigns by tuning their incident response process to treat all messages that belong to the same campaign with the same process.
- Static, gateway based tools lack the global visibility to gain this insight. Only cloud-based big-data analytics are capable of identifying the new generation of email-borne advanced threats.

But this is what we’re seeing – what has been your experience? Share your experiences in the Comments.

Tags: Phishing | Malware | Angler exploit kit

Post a Comment
Comments will be reviewed before being posted.
Your Name: 

Email Address: 

Comments: 

Submit

Related Posts

Training vs. Technology – what's best at stopping Phish-based Malware?

Attacks, Behavior, Data, Malware, Observations… Insight?

Nuisance Spam vs. Malware: can you tell the difference?