Surveillance Malware Trends: Tracking Predator Pain and HawkEye

researchcenter.paloaltonetworks.com/2015/10/surveillance-malware-trends-tracking-predator-pain-and-hawkeye/

Rob Downs October 16, 2015

By Rob Downs

October 16, 2015 at 3:00 PM

Category: Malware, Threat Prevention, Unit 42

Tags: AutoFocus, HawkEye, keyloggers, Predator Pain

Malicious actors employ a range of tools to achieve their objectives. One of the most damaging activities an actor pursues is the theft of authentication information, whether it applies to business or personal accounts. Unless specifically mitigated, this theft often allows an unauthorized actor to masquerade as the victim, either achieving immediate gains or creating a platform from which progressive attack campaigns may launch.

There are a number of threats that endanger the critical secrecy of credentials, including poor operational security practices, social engineering, man-in-the-middle attacks, password hash dumping and cracking, and surveillance malware. In this post, Unit 42 examines various trends in a malware threat set within the surveillance malware category: Predator Pain and its latest derivative, HawkEye.

Threat Background

Surveillance malware covers a broad range of capabilities, including:

- Capture of keyboard and / or input device (e.g., mouse) activity, with window / process awareness (keylogging)
- Taking asset display screen shots or video (display capturing)
- Assuming control of cameras and / or microphones attached to an asset (live surveillance)
- Interception of network communications (sniffing)

Each of these capabilities can be qualified by its scope (i.e., types of information collected) and method (ranging in techniques and sophistication). Additionally, some surveillance software includes its own exfiltration mechanism, while others may depend on external software to accomplish the transfer of captured information.

Both Predator Pain and HawkEye are considered **keyloggers**, but they also include additional features, such as web browser and e-mail client **credential dumping**, **display capture**, and **captured information exfiltration**. HawkEye is openly sold on a commercial website, whereas Predator Pain is usually acquired through underground forums. Associated features have made this set of malware popular with malicious actors across a number of motivations; however, the most prevalent motivation remains cyber crime, in which stolen information is directly exploited or sold for financial gain. (A list of additional reading links is found at the end of this blog post for anyone interested in learning more about this specific threat set.)

Trending and Analysis: July 2015-September 2015

The following sections describe Predator Pain and HawkEye trending and analysis conducted by Unit 42 from July 2015 through September 2015. We leveraged the Palo Alto Networks AutoFocus service, under which this threat set is tagged as **PredatorPain**.

Target Selection

Almost all of the adversaries Unit 42 observed employing this malware threat set harvest publicly disclosed or leaked e-mail addresses to construct phishing campaign targeting lists. These lists are mostly indiscriminant, with malicious actors seeking any opportunistic gains they can glean from "shotgun" style attack campaigns. The natural exposure of businesses with publicly advertised e-mail addresses (e.g., sales@<domain> or info@<domain>) makes for easy targeting of what typically represents key organizational e-mail distributions. In other words, these distributions normally reach a number of staff at the target organization who are motivated by their importance to business, increasing the likelihood of them inadvertently executing malicious code on their systems.

Threat Volume

Figure 1 depicts July to September 2015 sessions (individual occurrences) for this threat set.

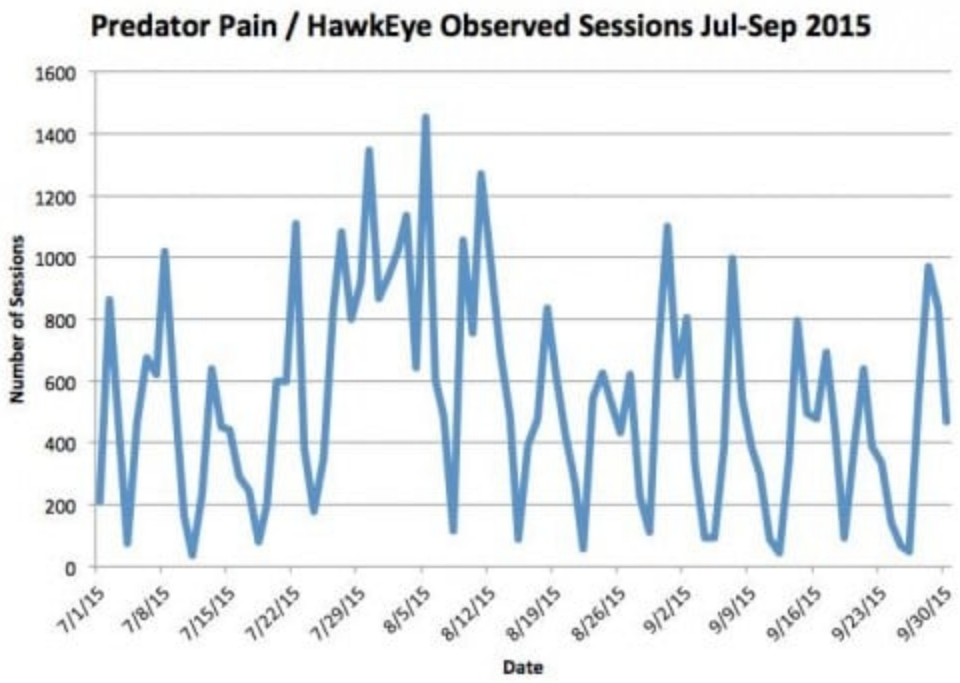

Figure 1: Predator Pain / HawkEye Sessions, Jul - Sep 2015

Observed sessions revealed an interesting pattern in distribution volume ramping up on Sunday for peaks over Monday through Wednesday, with significant volume dropping from Thursday onward. We believe this corresponds with focused business targeting early in the workweek, per the previously noted targeting process employed by most cyber crime actors.

Delivery

Figure 2 shows the delivery methods observed for the Predator Pain and HawkEye threat set over the period of interest, with e-mail by far being the preferred delivery method for adversaries.

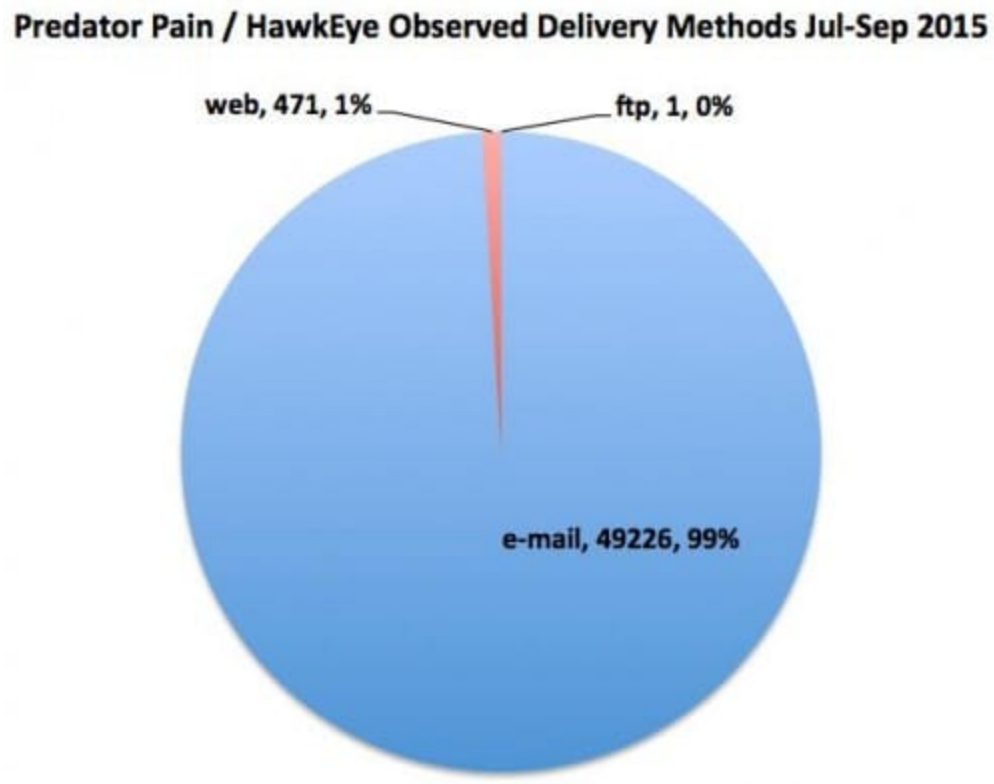

Figure 2: Predator Pain / HawkEye delivery methods, Jul - Sep 2015

Exploring respective phishing attacks further revealed the following lure themes:

- Notification or issues with product order or shipping
- Notification or issues with payment, purchase order, invoice, or billing
- Product or service quotation request
- Confusing, random, and/or purportedly personal topics

Table 1 contains some examples of more common e-mail phishing attack subject and attached filename pairings:

Email Subject	Email Attachment Filename
Re: Purchase Order	PO #5479423.exe
M.V. Chuetsu Spirit V.62A - SI / agency appointment / PDI	CHUETSU DREAM V.26A SI HK.scr
DHL AWB# 34 5673 0015 / shipment	payment.exe
New Order	ORDER.exe
Quotation.	purchase order.exe

Table 1: Lure theming examples for e-mail attacks, July - September 2015

Respective malware delivered via malicious e-mail mainly consisted of Microsoft Windows Portable Executable (PE) 32-bit and 64-bit binaries. Microsoft Word or RTF documents constituted the remainder of malicious files. Attempted downloads of this threat from web and FTP sites were also observed; however, these represented drastically lower occurrences (session counts).

Observed Targeting

With these distribution methods in mind, Figure 3 shows an AutoFocus visualization for the 80 countries Unit 42 observed as targeted by the Predator Pain and Hawkeye threat set during the noted time period.

Figure 3: AutoFocus view of Predator Pain / HawkEye targeted countries, Jul - Sep 2015

Not surprisingly, the top-ten list of most highly targeted countries includes 7 of the 23 wealthiest in the world, based on GDP per capita:

- United States
- Australia
- Canada
- Thailand
- Taiwan ROC
- Kuwait
- Japan
- Spain
- Italy
- Sweden

The top ten targeted industries accounted for 82% of sessions:

- High Tech
- Higher Education
- Manufacturing
- Professional and Legal Services
- Transportation and Logistics
- Wholesale and Retail
- Construction
- Media and Entertainment
- Telecommunications
- Government

We suggest three reasons based on this combination of observed countries and industries targeted:

- Innovative organizations are prime targets for a number of adversary motivations due to the capabilities and intellectual capital they aggregate.
- Service oriented businesses, striving to develop customer relationships are more likely to fall victim to phishing attacks due to both organizational culture and incentives for client and customer engagement.
- Natural target saturation occurs within countries with established or thriving infrastructure, enabling malicious actors to reach a broader range of targets remotely through technology.

Prevalent Malware Capabilities

The Predator Pain and HawkEye set of malware is feature rich, compared to most other keyloggers. The following are the capabilities Unit 42 observed as most often enabled for this threat set during the focal time period (ordered by prevalence):

- E-mail client credential dump
- Web browser credential dump
- Collection of system configuration information
- Logging of web browser activity
- Logging of e-mail activity
- Screenshot grabbing

Exfiltration Method Break-Out

This threat set includes three main methods of exfiltration: E-mail, PHP-based Web Panel, and FTP. Figure 4 shows the HawkEye keylogger's settings page, where the method employed by an instance can be specified.

Figure 4: HawkEye keylogger settings screen

The Predator Pain and HawkEye configurations analyzed by Unit 42 over the focal time period revealed the following break-out for exfiltration method, with e-mail constituting the preferred method across a number of malicious actors:

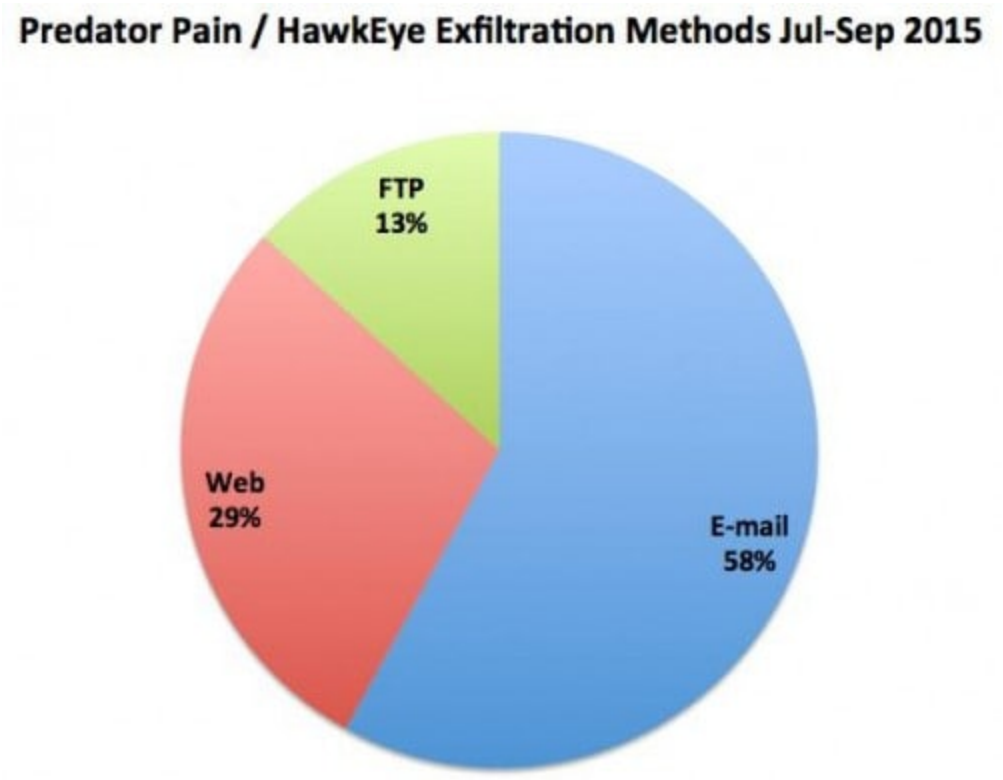

Figure 5: Predator Pain / HawkEye exfiltration method break-out, Jul – Sep 2015

Conclusion

Prevention is the best strategy when it comes to the threat posed by keyloggers, such as the Predator Pain and HawkEye set. System hardening, integrity assurance, software version and patch management, and user awareness are just the first steps towards threat mitigation.

Recommendations to protection against this class of threat include:

- **Employ multi-factor authentication:** Knowledge-based authentication relies on the secrecy of information. Including elements of what you have (i.e., hardware token) or what you are (i.e., biometrics) can reduce the value of respective stolen credentials for an adversary if that information only satisfies one level in the authentication process.
- **Limit the impact of stolen credential information:** Don't share credentials across accounts and change those credentials periodically. Adversaries commonly engage in activities such as credential stuffing in an attempt to maximize benefits of stolen credentials.
- **Maximize network control and visibility:** The latest Verizon DBIR included the finding that in over 25% of breaches, the organization was notified of the breach through a third party. Inbound, outbound, and internal network traffic needs to be controlled and monitored. This is also useful for disrupting malware C2 and exfiltration channels.

- **Integrate anti-malware automated dynamic analysis (e.g., sandboxing):** Identify previously unknown threats before they become much larger problems on the network. Given the anti-detection tools at the disposal of adversaries, this is a modern necessity.
- **Implement network segmentation:** Avoid flat networks, where once an adversary is in they have unrestricted access to internal resources. Network segmentation is a best practice for exposing only enough information as is required for specific organizational processes, moving toward a “zero trust” model. In this context, it is about further limiting the access of an adversary should they successful compromise credentials.

Additional Reading

The following are some analyses for the Predator Pain and HawkEye malware threat set that expand on associated capabilities, attributed actors, and observed campaigns:

- Palo Alto Networks: Examining a VBA-Initiated Infostealer Campaign
- Palo Alto Networks: Follow-On to VBA-Initiated Infostealer Campaign: Exploring Related Malware and Actors
- Stop Malvertising: Analysis of the Predator Pain Keylogger
- Trend Micro: Predator Pain and Limitless - When Cybercrime Turns into Cyberspying (PDF)
- iSIGHT Partners: HawkEye Keylogger Campaigns Affect Multiple Industries
- SophosLabs (via Virus Bulletin): MWI-5: Operation HawkEye (PDF)