WHITE PAPER

Fighting in the Cyber Ring

Be ready for the advanced threat

Advanced threats can quickly lead to knockouts when organizations are not properly prepared.

Many organizations believe that with standard security measures in place they are not at risk for an intrusion. But threat groups are ready for a fight. Follow these eight guidelines to help prepare for any cyber ring match.

1. Discretion is Key

Why? You will have a lot of people who have a vested interest in what is transpiring – from the Board of Directors, C-Suite, Legal Teams, IT Groups, etc. However, you are dealing with a targeted threat that is in your network where you are storing information that the adversary can potentially see. For example, an adversary can screen shot what you are talking about and alter their plan based on your incident response plans. The important thing to note is to have an established plan for out-of-band communications set up outside of your compromised infrastructure to ensure incident response efforts are not compromised by the threat group.

2. Don’t assume the fight is over and celebrate

Why? Say you have found the threat group. You develop a counter measure. Your security team is proud and wants to spread the word. What do you do? You share your findings publicly. What happens? The threat actor saw your public information and changes a characteristic to neutralize the existing countermeasure. This is why it’s important to make sure you don’t share anything publicly that will compromise the response. Ensure you finish the eviction and mitigate/ eliminate the threat before sharing any information that could compromise the response.

3. Be aware of the silent predator

Why? You have successfully evicted the threat actor. Things seem to be quiet and calm. You go back to normal operations. The fight was won and the threat is no longer a risk to your organization. Don’t be so sure. Threat groups are often persistent. Many times they are willing to stay quiet, play dead and hope that you won’t suspect a revisit. But they will come back...with new tactics such as registering new C2 domains and compiling new RATs just to name a few. It is important to always monitor for re-entry attempts.

4. Your organization may be collateral damage

Why? You are a victim of a security breach. You assume that the threat group's intent was to steal your organization's sensitive data. This may not be the case. It is important to understand the intent of the threat group to better prepare for the appropriate steps to defend against them. Your organization could be collateral damage from a threat group targeting someone or something different that is linked or adjacent to your organization. Ask questions to understand the intent. What information is on the system? What's the motivation? Who does this benefit and why?

The goal is to push threat actors back into a development model and make it inherently more complex to design a threat/exploit.

5. All fights are not the same

Why? You investigate and learn that there are multiple threat groups inside your network. Say for example there are three groups, each with different periods of access. How do you react? Take the same approach with one as the rest? Not necessarily. The key is determining if they are together. How do you know? Determine if they share tools, most threat groups do. Did each threat group conduct their own exploitation and infiltration or was there a single entry and then sharing of that exploitation/access? Additionally, determine what they are targeting. Does it look like it is a group effort to come to one final outcome or separate goals? In the case of multiple threat groups the one size fits all eradication and eviction process doesn't address the uniqueness of each threat group. Recognizing the different operating procedures leads to a more effective eviction. You may also be asking yourself, how do we plan for a specific threat group? In reality the question you should be asking is "When we read information about intrusions and how operations work/occur – if these tactics and tradecraft were used against my organization, how well could we defend against them?"

6. There may not be obvious tracks

Why? You assume that an adversary will access your environment using a remote access tool. However, say 21 employees received a phishing email asking employees to log into a website (thereby gaining credentials), one user clicked the link and entered their credentials into a fake access page, threat actors log into SSL VPN using the compromised account and conduct operations using legitimate sysadmin tools. They spread out across the environment and eventually exfiltrate via FTP. Point being, many times threat actors leverage legitimate remote access solutions to gain access to the environment. This makes detecting malicious activity much more difficult because the adversary is masquerading as a legitimate user. It is important to monitor for anomalous user activity.

7. Understand your adversary and where he is in his attack plan

Why? The threat actor got in and got what they wanted without you even knowing it. The damage was done by the time you tried to respond. You are not sure if the fight is over. So what do you do? You panic and assume the adversary is still operating in your environment. Instead, understanding where the actor is in the intrusion (what stage the actor is at) is important to guiding your response. It is important to scope the activity to understand at what point in the fight you are getting involved. Your response will change based off whether the fight just started, has ended, or is ongoing.

8. Give it all you’ve got

Why? You are under attack by an advanced threat actor. So what do you do? You assume that your normal mitigation plan will be effective. Unfortunately, you may just be seeing the tip of the iceberg. It is better to act with urgency and fight rather than assume traditional security controls will keep you safe.

Lessons Learned

- Establish offline/out-of-band communications
- Finish eviction before publishing findings
- Maintain vigilance to catch re-entry
- Understand you may not be the target
- There may be more than one threat group operating in your environment
- Look for points of access, not malware
- Threat group decides length of fight
- Investigate targeted intrusions, not events
- Different organizations have different motives, methods, and sources for threat groups

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp