The Power of a Tailored Threat Model
By any measure, the group known as APT10 (aka “Stone Panda,” aka “MenuPass,” aka “Red Apollo”) is an “advanced threat actor.” Active since at least 2009, the People’s Republic of China-based hacking group has been linked to attacks on some of the West’s top government agencies and companies in industries including defense, aerospace, and heavy industry.

So dangerous is the group, that the UK’s National Cyber Security Center, part of the Government Communication’s Headquarters (GCHQ), issued a warning to UK companies specifically describing the group’s campaign against global MSPs (managed services providers) on six continents, which gave it access to the networks of top firms. In the U.S., the Department of Justice filed an indictment in December 2018 naming two of the group’s members, Zhu Hua and Zhang Shilong, and charging them with a string of crimes including conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft.¹

What makes a group like APT10 an “advanced threat actor” has more to do with the sum of its actions, operations, and tools than any one element or method of attack. Advanced actors are resourceful, resilient, and nimble as they work at compromising and maintaining access to the organizations they target, even if their tools and techniques are not advanced or sophisticated. The group’s resourcefulness, flexibility, and patience in carrying out operations makes it difficult to spot, and at times even more difficult to eradicate once compromised.

Understanding both the modus operandi of a group like APT10 – its tactics, techniques, and procedures (TTPs) – is necessary, but not sufficient to thwart damaging attacks. Organizations must also be able to put that threat information into context for their environment(s) including their network, data, staff, business partners, and supply chain. By understanding not just how a threat actor behaves and what types of organizations it targets, but also how your organization is uniquely exposed to that threat actor, you can begin to get ahead of threats instead of reacting to them.

¹ FBI [https://www.fbi.gov/wanted/cyber/apt-10-group](https://www.fbi.gov/wanted/cyber/apt-10-group)
² GCHQ [https://www.ncsc.gov.uk/alerts/apt10-continuing-target-uk-organisations](https://www.ncsc.gov.uk/alerts/apt10-continuing-target-uk-organisations)
Traditional Defenses Don’t Cut It //

To respond to these more nimble, patient, and resourceful hackers, most organizations are left to choose among traditional forms of threat defense. These include perimeter-based defenses like firewalls and email gateways, intrusion detection and prevention software, data leak prevention, endpoint security tools, and so on.

These tools, taken separately, are powerful and effective at what they are designed to do. But for organizations that hope to thwart sophisticated threat groups like APT10, an IT-centric “detect and block” approach is inadequate to the task.

Public accounts of APT10’s activities suggest why. Reports by PricewaterhouseCoopers and BAE Systems³ document the group’s use of a variety of techniques that were both sophisticated and unsophisticated in nature. Spear phishing attacks against employees at target organizations were unsophisticated: emails with archived (RAR) attachments containing .lnk files or executables using “double” file extensions (so: “phishyfile_doc.exe”).

But APT10 didn’t stop there. Analysis of recent campaigns show that the attackers were willing to “go the extra mile,” by compromising third parties and MSPs, and then leveraging their access to the compromised MSPs to gain trusted access to the ultimate target: the MSPs’ customers. Among other things, APT10 deployed a well-known backdoor, dubbed “SOGU” on the MSP’s network and then used the system it was deployed on as a proxy, masking malicious C2 and exfiltration traffic from the victim network.

Additionally, APT10 was observed using novel malware in its campaigns, including tools like HAYMAKER, a backdoor program that can profile victim systems, and BUGJUICE, a backdoor that can canvass networks: finding files, enumerating drives, stealing data, and even capturing screenshots of infected systems. Once developed, custom malware such as these are guaranteed to slip by traditional anti-malware and endpoint scanning tools. Assuming the tools are not widely deployed, they might persist for days, weeks, or even years disguised as legitimate or benign applications. Threats that can't be detected can't be blocked, leaving victims vulnerable to data theft and predation.

Modern Defense is Holistic, not Targeted

APT10 shows us why point-protection based approaches and “detect and block” tools are inadequate to the task of blocking advanced threat actors. More and more, organizations are embracing a holistic approach to threat defense that encompasses protection from multi-vector attacks like those used by APT10. This approach accounts for both the prevalence and importance of social engineering (spear phishing) attacks and the use of “fileless” attack methodologies that leverage common system management tools to extend attackers control over victims’ environment.

Critical to holistic cyber defense is taking a “whole company” approach to defense. This means considering the IT assets and data owned and managed by the firm as well as third party software and service providers, business partners, current and former employees, and customers.