Trend Micro Incorporated
Opinion Piece
September 2012

# Peter the Great Versus Sun Tzu

Tom Kellermann
Vice President of Cybersecurity

*The author would like to give special thanks to the Forward-Looking Threat Research E-Crimes Division at Trend Micro, Inc*

While East Asian hackers dominate cybersecurity-related headlines around the world with high-profile intrusions and advanced persistent threats (APTs), it would be a mistake to conclude that these attackers are the sole or greatest criminal threat to the global Internet today. After conducting extensive research into the nature of the East Asian and East European underground, Trend Micro has concluded that hackers from the former Soviet Bloc are a more sophisticated and clandestine threat than their more well-known East Asian counterparts.

Peter the Great is now manifesting himself in cyberspace. To understand this phenomenon with greater clarity, one must recount some history.

One of Peter the Great's notable innovations was his strategic decision to allow virtually anyone from among the rank-and-file to reach high ranks in the Russian military. Young nobles would often begin service alongside commoners; those who distinguished themselves would reach high ranks, whether commoner or noble. This stroke ensured that men of ability would lead Russia into battle and was a key component of his modernization of the Russian military. One of Peter the Great's great military achievements was his ability to change the geography of the battlefield. Locked in a war with Sweden, Peter seized Swedish holdings on the Baltic Coast, including a small fort, Nyenskans. The fort was renamed St. Petersburg and, 10 years later, it was declared the capital of the Russian Empire. Peter the Great took Swedish territory and made it his own, not only with bold military maneuvers but also through colonization, to ensure it would never be Swedish again.

American enterprises are being colonized in cyberspace. Trend Micro has concluded that East European hackers pose as much of a threat to enterprises as their more well-known East Asian counterparts. Six core conclusions from ongoing research into the East European underground support this conclusion:

- **More sophisticated malware:** East European hackers tend to use custom-built, highly complex malware; East Asian hackers are persistent but use more off-the-shelf malware and simpler techniques.

- **More sophisticated infrastructure:** East European hackers carefully choose bulletproof hosters and use their own infrastructure; East Asian hackers use cheap hosted infrastructure at mass-hosting Internet service providers (ISPs), for example.

- **Mercenary commandos versus organizational foot soldiers:** East European hackers are professional "guns for hire" working in small, tightly knit teams that directly derive profit from their actions; East Asian hackers work as part of a larger legion of hackers at the direction of large institutions that provide material support as well as direction.

- **Markedly different focus:** East European hackers focus on credential theft; East Asian hackers focus on stealing sensitive corporate data.

- **Reputation is king:** East European hackers' individual reputations impact their ability to directly profit from their work; East Asian hackers rely less on individual reputation for profit and more on the material support of the institutions they work for.

- **Difficult to detect:** East European hackers operate in a competitive, specialized marketplace and therefore take great pains to heavily camouflage their activities; East Asian hackers are aware they are "one among many" and do not fear disclosure of their intrusions.

These conclusions are explained in more detail below.

## More Sophisticated Malware

Due to the competitive nature of the environment, East European hackers create customized malware, often with all capabilities internally hard-coded with no external third-party tools. Trend Micro threat researchers noted that robust anti-debugging techniques and complex command and control (C&C) are hallmarks of East European design. East European malware are not always innovative but often incorporate several exploits designed by others in creative ways. An East European hacker is only as good as his last successful job. East European malware are so elegantly crafted, they have been dubbed the "Faberge Eggs" of the malware world. This is due in part to the long history of high-quality science and math education in the former Soviet Bloc. With the fall of communism and the free market chaos that ensued, East Europeans with strong math and science backgrounds turned to the skills developed to help fight the Cold War and started using them to put food on the table by selling them to the highest bidder. In addition, computer scientists in the former Soviet Bloc had to make do with simpler, less sophisticated computing resources, which instilled in them a discipline to make every line of code count. These were combined to yield a pool of expert craftsmen able to build high-impact, small-footprint malware. Probably the best recent example of this is in the new Tinba malware—a well-crafted piece of malware that is optimized for size and capability and used in Trojan banker attacks targeting Turkey.

In contrast, East Asian hackers normally use really basic malware that "do what they need to do," according to one Trend Micro threat researcher. As speed and ultimately productivity are of the essence to East Asian hackers, fewer anti-debugging techniques exist, East Asian backdoors are simpler and often only a minimum of C&C is required to maintain remote persistent access is present in the code. Often, East Asian malware are thrown together quickly using already-existing components. A second researcher summed it up, "There are certainly a lot of elite East Asian hackers who are capable of very dangerous attacks... [but] East Asian hackers seem to be a bit less sophisticated." Because East Asia is a more recent entry into the global high-tech marketplace, part of this approach can be due to the lack of native in-country capability like you see in East Europe. East Asian hackers are determined to get a piece of the global criminal enterprise pie but have to beg, borrow, and steal some of the means to do so.

## More Sophisticated Infrastructure

East European hackers tend to develop their own infrastructure specifically for their own use in attacks. They tend to want to be in control of their entire infrastructure and will routinely set up their own servers for use in attacks as well as develop their own Domain Name System (DNS) servers to route traffic and create sophisticated traffic directional systems for attacks. If they do go outside, they will carefully select bulletproof hosters to support their infrastructure. It is their hallmark to maintain control of the whole stack similar to the business models pioneered by Apple. This quality commands a premium price and RuNet the East European "arms bazaar" tends to enjoy providing weaponry to the masses for a fee versus the East Asians who like to use generic mass-produced malware.

East Asian hackers, on the other hand, tend to use cheap, hosted infrastructure usually from mass ISPs that are easy to set up and manage. They are not necessarily concerned with being identified as the attackers, as they do not go to great lengths in hiding their tracks like East European hackers do. This was shown in the recent Luckycat incident, which was traced back to Sichuan University—a known training school for East Asian military.

## Mercenary Commandos Versus Organizational Foot Soldiers

East European hacker crews operate like mercenary commando units. They organize themselves into small, tightly knit, independent units that make their living by selling their services to others. Like mercenary units, less-skilled or sophisticated actors provide common, basic services and command less of a premium while expert, specialized resources can charge higher rates in the marketplace.

Like mercenaries, East European hacker crews survive and thrive based on their accomplishments. The more they "kill," the more they make. Because of this, they are more precise and focused in their attacks, for instance, performing significant reconnaissance on their targets prior to beginning their cyber-kill chain. An East European hacker crew that fails to deliver cannot expect to survive for long.

East Asian hackers, on the other hand, tend to be cyberfoot soldiers who are charged with gathering usable data for their commanders rather than obtaining "sellable" data. They tend to be employed by another organization interested in using their skills. Because they work as part of a larger organization that provides material support, East Asian hacker crews can focus less on immediate financial success in favor of longer-term strategic gains. Given material support and direction from the institutions they work for, East Asian hackers are more insulated from the losses around failure as well as the gains around success. One of the best examples of this is the role played by an East Asian foot soldier in the Luckycat APT campaign.

## Markedly Different Focus

Consistent with the need to support themselves as mercenary commando units, East European hackers focus on profit and stealing data they can sell or use within their underground market. East Asian hackers, on the other hand, tend to focus on grabbing as much data as they can. This appears to be driven more by the goal of obtaining information, which will help further the competitiveness of the state in the global economy than making the hacker profit.

## Reputation Is King

This statement can be summed up by the following quote from a Trend Micro threat researcher, "If an East European attacker gets defaced, he is out of business. If an East Asian attacker gets defaced, he is still employed and his employer uses him in another attack." The East European underground is a tightly knit community of fellow mercenary commandos who routinely buy and sell data to one another. If your reliability is called into question, your ability to profit or even survive is harmed, possibly to the point of extinction. In contrast, East Asian hackers rely on the organizations they work for in terms of material support. To them, reputation is less important than being part of a good, strong, established organization.

## Difficult to Detect

Like one would expect from a team of mercenaries who focus on profit and need to maintain a good reputation, not getting caught by preventing detection is a key concern. In general, one can say that East European attackers are "technology drivers" in detection prevention. They come up with elegant new techniques in each of their staged attacks to enable them to further their goals while minimizing detection. East European remote access Trojans (RATs) have all of their capabilities internally hard-coded. They do not use external, third-party tools. For example, password hash-dumping is performed by an internal function. Thus, a pass-the-hash toolkit is not required. The malware is a one-stop shop of capability in the network. This shows a significant differentiation between East Asian and East European groups.

Since detection is less of a concern, East Asian attackers tend to reuse proven technology created by others and hide in plain sight. Their backdoors are simple in nature, doing only the minimum of C&C required to maintain remote persistent access. Once access is gained to the network, the East Asian APT is largely about lateral movement, use of command-line tools, and passing of credentials. These tactics can be seen in the IXESHE (pronounced "i-sushi") APT campaign where attackers focused on techniques to better enable lateral movement on compromised networks. The thousand-grains-of-sand approach is symbolic of an East Asian colonization, as reconnaissance is ongoing and the battlefield not necessary prepped like the East European model.

Per the cyber-kill chain itself, East Europeans heavily focus on credential theft and enjoy using distributed denial-of-service (DDoS) attacks and "Syrypt" (i.e., encryption for the purposes of extortion).

East Europeans heavily focus on targeting financial Institutions and thus have developed cybermoney-laundering systems that vet their customer base and act as alternative payment channels. The recent explosion of man-in-the-browser attacks like Tinba are evidence that East Europeans are laser-focused on the financial sector and are creating automated nano-malware to grow their shadow economy.

## Tactical Comparison of East European and East Asian Hackers

| Hackers | East Europe | East Asia |
|---|---|---|
| Patriotic hackers<br>**Goal:** Support their homeland | Website defacement; ability to conduct large-scale DDoS attacks; coordination with military operations (RU-GE War) | Website defacement; ability to conduct large-scale DDoS attacks |
| Criminal hackers<br>**Goal:** Generate profit | Profitable operations with affiliate model distribution and active underground economy; professional malware development; professional exploit pack development; global distribution and mass targeting | Profitable operations with "cell" structure and active underground economy; primarily focuses on China |
| Espionage hackers<br>**Goal:** Steal intellectual property | Still not well-known; possible operation leveraging criminal tools and infrastructure (ZeuS/Kneber); possible "APT-style" operations emerging with good operational security | Development and use of advanced exploits, including zero days; highly targeted attacks; low-quality malware or use of publicly available malware (RATs); persistent operations with low operational security |

| Evolution | East Europe | East Asia |
|---|---|---|
| Patriotic hackers | Increasingly organized around political lines since the DDoS attack against Estonia; willing to initiate the "first strike" | Increasingly reactive to attacks against East Asia; less likely to engage in "first-strike" attacks |
| Criminal hackers | Focus on credentials, especially banking; increasing awareness of the value of other data (i.e., sensitive information) | Increasing professionalization and targeting outside East Asia |
| Espionage hackers | Movement from using ZeuS in somewhat targeted attacks (e.g., Kneber) to APT-style malware and more precise targeting (still a bit unclear) | Increased production of new but functionally similar, low-quality malware; engaging in both broader targeting (i.e., industry) alongside highly targeted attacks (i.e., individual or company) |

## Conclusion

In sum, one could say that East Europe is a high-end market while East Asia is a mass market when it comes to hacking. In general, East Asian hackers do not have the same level of maturity in terms of skill as their East European counterparts. East Europeans are master craftsmen who have developed a robust economy of scale, which serves as an arms bazaar for a myriad of cybermunitions and bulletproof hosting infrastructure. East Europeans act like snipers when they launch campaigns whereas East Asians tend to colonize entire ecosystems via the thousand-grains-of-sand approach.

The Trend Micro Forward-Looking Threat Research Team routinely analyze the many different criminal undergrounds to learn their tools and techniques in an effort to help build better ways of identifying new threats. This "threat actor intelligence" is part of the correlated global threat intelligence used by Trend Micro products and services through the Smart Protection Network™. Effective cybersecurity is dependent upon situational awareness and a CISO's ability to learn from history and spin the virtual chess board. In order to manage cyberrisks in 2012, one must pay homage to the strategic genius of Peter the Great.

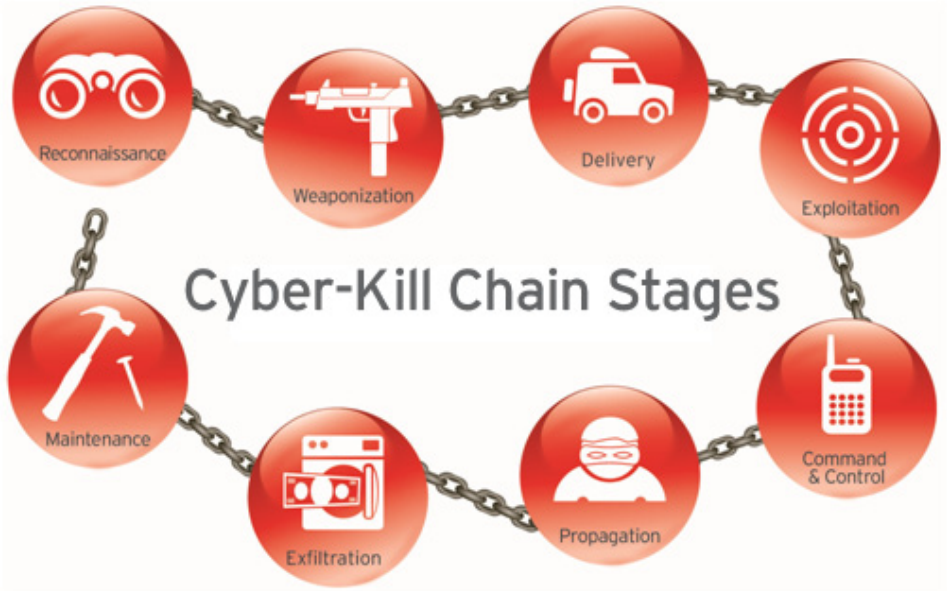
As Vice-President of Cybersecurity at Trend Micro, Mr. Kellermann is focused on acting as a trusted cybersecurity advisor and strategist within the federal, financial markets.

Tom Kellermann served as a Commissioner on The Commission on Cybersecurity for the 44th Presidency and serves on the board of the International Cybersecurity Protection Alliance (ICSPA). He sits on many boards, including the National Board of Information Security Examiners Panel for Penetration Testing, the Information Technology Sector Coordinating Council, and the Information Technology Information Sharing and Analysis Center (IT-ISAC) Subcommittee on International Cybersecurity Policy.

Formerly holding the position as Chief Technology Officer and Chief Cyber Strategist at AirPatrol Corporation, Tom Kellermann also spent five years as Vice President of Security Awareness for Core Security.

Previously, he was the Senior Data Risk Management Specialist for the World Bank Treasury Security Team, where he was responsible for internal cyber-intelligence and policy and for advising central banks around the world about their cyberrisk posture and layered security architectures. Along with Thomas Glaessner and Valerie McNevin, he co-authored the book "E-Safety and Soundness: Securing Finance in a New Age."

## The Cyber-Kill Chain




### TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

### TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud