

Checking in with Stonesoft on CyberSecurity Issues

There are some that would interpret the Homeland Security Department data on cyber attacks as a sign of a new growth industry, but with corporate, personal and other key data at stake it's no laughing matter. I recently spoke about this with Brian Vosburgh a solutions architect at Stonesoft, Inc., a provider of network security and high availability solutions to thousands of enterprises and government agencies across the globe. Unlike other vendors, Stonesoft focuses 100 percent on developing "military grade" network security solutions that simplify management and protection.

VERSACE: *Brian, there have been numerous reports of cyber attacks in the last few months. For those who are not aware, what are cyber attacks and what are some of the threats they pose?*

VOSBURGH: A cyber attack is a computer-based attack on corporate, personal, government and other computer-based information and systems. Hackers, which range from a single individual to organized groups, are typically motivated by financial gains or political influence.

The threats posed by cyber attacks exist on many levels - ranging from national security to identity theft. For example, in June 2010, the Stuxnet worm crippled industrial systems in Iran. Many believe this was a politically-motivated cyber attack to prevent uranium enrichment at research facilities. Another example are the Sony Playstation attacks that occurred in April and October of this year, resulting in a data breach that compromised personal data for more than 100 million online gaming accounts.

VERSACE: *How does a business arm itself against such attacks so it is prepared, not just responding to these attacks?*

VOSBURGH: A layered approach to network security, equipped with an accurate and centralized view of network activity, is the best approach. Having a firewall is no longer enough. Companies need to protect themselves from incoming threats that originate outside of the organization as well as from internal threats originating within the organizations. With an increasing number of employees accessing sensitive information on their smartphones and tablet devices, companies must also protect themselves against the threats inherent with remote access.

Most importantly, companies must protect themselves against human error. A few years ago, Gartner concluded that 99% of network attacks were due to human error (specifically, how devices are configured). This is no surprise as network security has become such a complicated piece of IT. Companies need to identify solutions that protect AND simplify network security management including the automation of routine tasks, updates and upgrades.

STONESOFT

Network Security

StoneSoft, Inc. - Founded in 1990, Helsinki based Stonesoft Corporation (NASDAQ OMX: SFT1V) is an innovative provider of integrated network security solutions to secure the information flow of distributed organizations. Stonesoft customers include enterprises with growing business needs requiring advanced network security and always-on business connectivity. More on the company can be found at www.stonesoft.com

VERSACE: *What are the top 3 cyber security concerns a CEO should know about?*

VOSBURGH: There are really four concerns that every CEO today should be discussing with their IT teams. Advanced evasion techniques, human error, cloud security and mobile security.

1. **Advanced Evasion Techniques:** The sophistication of cyber attacks is growing by leaps and bounds. Last year, Stonesoft discovered an entirely new category of threats called Advanced Evasion Techniques (AETs) that can bypass nearly every network security device on the market today. In an age where a security breach can cripple both corporate productivity and reputation, this begs a question that every CEO should be asking their IT leaders: What are we doing to protect against the most advanced security threats?
2. **Human Error:** Most hackers access networks not because of inadequate security, but because inadequate management of security. When a network administrator misconfigures a firewall (or any other network device), they open the network up to attack (see Gartner stat above).
3. **Cloud Security:** With more and more companies hosting critical business information in the cloud, CEO's need to understand how these assets are being protected.
4. **Mobile Security:** Smartphones and tablet devices are changing the way we do business. But they are also exposing the corporate network to new threats as these devices often combine personal and professional identity and data.

VERSACE: *When we look at cyber security, who are some of the key players addressing this market?*

VOSBURGH: Well, it depends on what aspect of security you're talking about. There are anti-virus players, like McAfee and Norton. Then, there are network infrastructure players like Juniper and Cisco who got their start on the network infrastructure side (i.e. routers, switches) and began offering security solutions later. Finally, there are pure-play network security vendors like Stonesoft that focus solely on network security and who provide a solution that has been purpose built for network security rather than "development by acquisition".

VERSACE: *Because Stonesoft is yet to be a household name here in the U.S., share a brief description of the company and its strategy.*

VOSBURGH: For the past decade, Stonesoft has provided network security and high availability solutions to thousands of enterprises and government agencies across



the globe. The company operates globally and is headquartered in Helsinki, Finland with U.S. offices in DC, Atlanta and New York. Unlike other vendors like Cisco, Stonesoft focuses 100% on developing "military grade" network security solutions that SIMPLIFY management and protection.

VERSACE: *What distinguishes Stonesoft from others serving the network security market? How does the company compete and win?*

VOSBURGH: Organizations turn to Stonesoft because we provide military grade protection. Think about it - the average large enterprise network has hundreds of firewalls and other network devices that must be configured every time a new virus or threat is discovered. So, not only do they need the highest level of security, they need to be able to easily manage security across the network. Stonesoft does this better than anyone else by giving administrators the tools to centrally monitor and manage their entire network security infrastructure from a single management center - this includes virtual and physical devices as well as the monitoring of other vendor devices using our technology. We also provide security that is context-aware. That means that our solutions know who is accessing the network, how they're accessing it, from where and what applications they're using. This is the type of information that helps IT make better decisions about where, when and how they need to improve security across the network.

We're able to do this because we employ some of the brightest researchers and developers in the world. Last year, our research team discovered a new category of cyber threats called Advance Evasion Techniques. Today, other researchers, testing labs and global IT consultancies are using this research to stay a step ahead of the next generation of attacks.

VERSACE: *Per recent financial reports, Stonesoft is delivering double-digit top line growth. How and why is Stonesoft taking market share?*

VOSBURGH: We believe that security is a process, not a technology. For Stonesoft, part of that process is industry leading research and development focused on advancing both our own technology and setting the pace for the industry. The most obvious example of this is our Advanced Evasion Techniques (AET) research, which has been a catalyst for rethinking network security performance and intelligence. With the industry labs now incorporating AET protection into testing requirements, and network security vendors incorporating Stonesoft's Anti-Evasion Readiness Tool in their own testing, we see market share expanding to include other network security vendors as well as new customers wanting to be prepared. This is exciting news for us, but it's also indicative of how the network security industry is functioning today. Those security companies that focus on delivery true innovation and improvements are experiencing fast-paced growth. Those whose focus is distracted, lack innovation, or rely solely on their brand name and size can no longer excel as they have in the past.

For Stonesoft, our most significant growth in both the US and Europe has

been in the public sector. This is in large part to our competitive edge and experience in this market, in addition to: AETs; regulations such as NIST's Continuous Real-time Monitoring requirements, which our management platform addresses very well; and recent cloud initiatives that our virtual solutions support. By continuing to provide flexible and high performance solutions that simplify deployment, management, and the costs associated with network security, we feel very well positioned to maintain growth.

VERSACE: *I see that Stonesoft is growing its headcount. In what geographic markets and business functions is the company expanding?*

VOSBURGH: Stonesoft is investing in the US commercial and federal markets. We have expanded our federal sales team based out of our DC office and basically doubled our entire US organization.

Specific market expansions include a Managed Service Partner (MSP) and Managed Security Service Partner (MSSP) program as well as our A2Cloud initiative that provides secure access to the cloud.

VERSACE: *With headcount rising and R&D expenses high as a percentage of sales, what is the company's target operating model? How does it get there?*

VOSBURGH: We get there by leveraging our partner networks with a few key large US partners that have the scope and reach as well as the experience working with large organizations and the federal government.

VERSACE: *Aside from market drivers, is there anything on the regulatory horizon that could prove beneficial to Stonesoft?*

VOSBURGH: Federal cloud initiatives and NIST's Risk Management Framework (specifically the Continuous Monitoring requirements). Both of these require public sector organizations to increase both network security and network security management capabilities - which is exactly where Stonesoft has demonstrated exceptional capability and success.