# Beyond Security Issues Statement on Petya, Massive Ransomware Attack in Europe

CUPERTINO, CALIFORNIA, USA, June 28, 2017 /EINPresswire.com/ --

Beyond Security
19925 Stevens Creek Blvd.
Cupertino, CA 95014
For Immediate Release

Cupertino, CA June 27, 2017 – Beyond Security, a leading provider for automated security testing solutions including vulnerability management released a statement regarding more information on the latest cyber ransomware attack to hit hard in Europe.

Petya or NotPetya is a new and evolved form of attack that is affecting many governmental and non-governmental entities throughout the world and particularly in Europe. Merck pharmaceutical, Chernobyl radiation detection systems, the Kiev metro, advertising giant WPP, French construction materials company Saint-Gobain, Russian steel and oil firms Evraz and Rosneft, an airport and many banks have been affected. The pernicious nature of Petya makes it deadlier than WannaCry that recently made news.
“This new form of ransomware seems to have evolved from the previous versions though it relies on the same leaked NSA tool called EternalBlue,” said Hamid Karimi, VP of Business Development at Beyond Security. “Petya boasts certain features that allows it to rapidly spread across networks by stealing credentials such as passwords on infected computers' storage and even by eavesdropping on residual data in memory” he added.

The NotPetya malware also exploits a weakness in Windows Management Instrumentation (WMI) to access relevant data and compromise other machines. Petya ransomware encrypts the master boot records of infected Windows computers, making affected digital assets inaccessible by exploiting vulnerabilities in the Server Message Block (SMB).

What makes the current computer pandemic more dangerous is its ability to use combined weaknesses and infect partially patched systems or even endpoints that are running the newest version of Windows (Windows 10).
“The widespread nature of this attack indicates that the operation's target is indiscriminate and is not necessarily aimed at a specific segment; it just happens that larger organizations that do not adhere to the security best practices leave gaps behind which are masterfully exploited by such malware. It goes without saying that using unpatched and unsupported software increases the risk of proliferation of cybersecurity threats such as ransomware” Hamid Karimi emphasized.

Service providers have begun to react and unilaterally block the communication path with the attackers; the German email provider Posteo severed the link between the compromised users and the ransom collectors to neuter such digital terrorism and remove the incentive for future abuses. Similar actions can be expected by other providers in the near future. In brief, the easiest approach for companies is to deploy preventive security tools such as vulnerability assessment to avoid getting blindsided by malware attacks.

Beyond Security is a leading worldwide security solutions provider. It's testing tools accurately assess and manage security weaknesses in networks, applications, industrial systems and networked software. Beyond Security's product lines include, AVDS for network vulnerability management and beSTORM for software security testing, which can help secure network and applications and comply with the security policy requirements that exceeds industry and government standards.

Founded in 1999, Beyond Security's solutions are essential components in the risk management program for many organizations worldwide. With the headquarters located in Cupertino, California, Beyond Security's distributors and resellers can be found in North and South America, Europe, Asia, Africa, the Middle East and Australia.
For more information, please contact – Sonia Awan at 747-254-5705 or at soniaa@beyondsecurity.com
Or visit us at www.beyondsecurity.com and https://blogs.securiteam.com/

#####

Sonia Awan
Beyond Security
747-254-5705
email us here

---