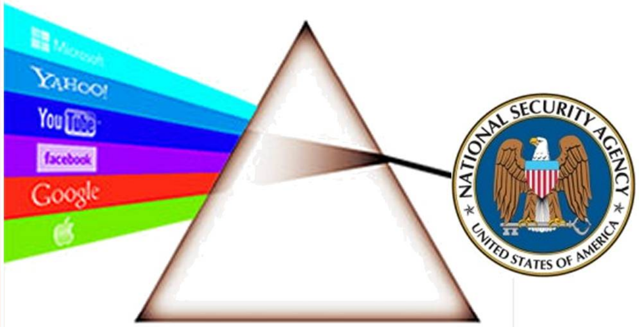
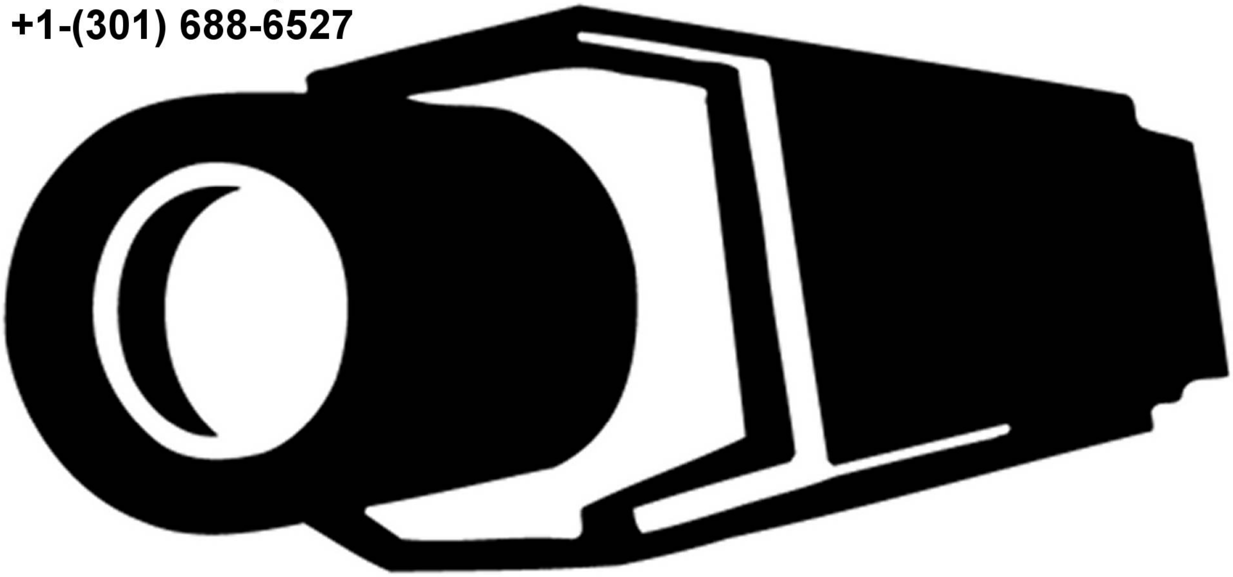
CDM
CYBER DEFENSE MAGAZINE™
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

JUNE 2013



FOR A GOOD TIME, CALL:
+1-(301) 688-6527



WHEREVER YOU GO, WHATEVER YOU DO, WHOEVER YOU ARE,

YOU ARE UNDER SURVEILLANCE

Why are ERP systems an easy target for cyber-attacks?

by Alexander Polyakov CTO at ERPScan

At first, cyber-attacks are real and their number is going to grow. While filtering all information on this topic, I paid attention to the special area, which is related to cyber espionage and fraud. Among the most recent interesting findings, there was an AutoCad worm that steals files with interesting drawings and sends them to China. We are talking about real targeted attacks focused on stealing corporate secrets here. It's not a simple example: there are many worms looking for PDF files with interesting content and sending them to authors, but this AutoCad example is something that can be a start of a new type of cyber-espionage weapons. All of this must be taken into account because there is one area which is underestimated in comparison to the current top security topics such as Cloud, BYOD and SCADA. Nowadays, the targets are mostly countries and their critical infrastructure, but there are business applications such as ERP systems that store and process critical data. They can become the target of espionage and fraud while very little attention is paid to them now. For example, there are a lot of internal fraud attacks, but should such an attack be automated and combined with a worm that would deliver exploits to the ERP system, you will combine the risk of a single fraudulent action with the power of the computer worm, which may potentially lead to the financial collapse of a single country if, for example, money from all financial organizations is simultaneously transferred to a certain account by this worm.

An ERP system is the heart of any large company; it enables all the critical business processes, from procurement, payment and transport to human resources management, product management and financial planning. All data stored in ERP systems is of great importance, and any illegal access can mean enormous losses, potentially leading to termination of business processes. Our "SAP Security in Figures" survey shows that the situation has changed significantly since early 2000s, when nobody knew about vulnerabilities and there were only fractions of information about them. In 2000, all the security of SAP boiled down to segregation of duties. By 2012, the interest in SAP has grown immensely in the security community, with 20 unique reports being released per year about various research in this area. SAP AG also started paying a lot of attention to this area, increasing the security of their products and conducting internal security conferences with external guest experts. We are working closely with them on discovering and patching security issues, so the process is underway. But the main issue is that the responsibility for securing business applications now falls to administrators, who should implement all applications securely, take customization into account and prioritize security updates. SAP itself can be securely configured, but it is not an easy task, especially if you do it manually and deal with a lot of systems. We also need to understand that SAP is not the only solution: there are Oracle and Microsoft business applications, and their security is no better.

ERP is a perfect target for cyber weapons because it is much easier now to find bugs and to exploit them, comparing to OS or browsers. Those are the targets of many cybercriminals and it is harder with every year to find something useful. ERP systems also store all data that you need so you do not need to design special payload or complex exploits such as Stuxnet. Speaking about the attacks that were described in public, the hot news from November about Anonymous attack on Greece finance ministry are worth remembering. They used an exploit on the SAP system and published critical inside documents. While this information is neither approved nor declined, it's a sign of interest in this topic anyway. Not only hacktivists but other large companies, too, can be interested in attacks on ERP, stealing corporate secrets, or executing DoS attacks on a competitor's infrastructure. I spoke to some commercial organizations that sell and buy exploits for private and government companies (security intelligence services), and I was interested if there is a market for ERP exploits. They say that there is interest from both sides. Also, there are forums that sell access to botnets with IP ranges of specific companies. Nowadays, large companies sometimes have more power than governments, so corporate wars are one of possible scenarios, and business critical systems can be the most useful targets. And if no examples have been made public yet, in most cases it is because very few organizations use at least something to monitor malicious activity, so even if their system was compromised, they are not ready for forensic investigation and cannot expose the fact of compromise.

We are trying to increase awareness in this area. Put all threats together and design the best approach. For example, there are a lot of areas which should be analyzed such as backdoors in custom source code or logging of all relevant events for forensic investigation. Putting it all together and combining different methods, we also collect information for the project OWASP-EAS which is focused on the security of business-critical applications. Speaking of automated solutions and commercial software, technical assessment appeared in the end of 2010/11 while SoD checks were known since 2003. Nowadays, there are some players in the area of vulnerability assessment and SAP security monitoring focused on preventing cyber-attacks, including our company, of course. We are unique in ensuring full coverage of SAP security, including vulnerability assessment, source code security review, SoD, monitoring of malicious activities and attacks. As I said before, we cover business and technical areas that allow us to see the whole picture and understand more. It is like 1+1=3. It is a pretty small market yet, but we see great potential and a number of new competitors appear.

About The Author

Alexander Polyakov is CTO of ERPScan. Co-founder of ERPScan. Organizer of ZeroNights, a deeply technical security conference. Expert in security of enterprise business software like ERP, CRM and other. Manager of OWASP-EAS. Well-known security expert in SAP and Oracle security, who published over 100 vulnerabilities in the applications of these vendors. Writer of multiple whitepapers and surveys devoted to information security research in SAP, for example, the award-winning survey "SAP Security in Figures". Alexander is frequently invited to speak and train at prime international conferences such as BlackHat, RSA and 30 others around the globe as well as in internal workshops for SAP and Fortune 500 companies. Alexander can be reached online at @sh2kerr and at company website http://www.erpscan.com/