ASIA'S FOREMOST INFORMATION SECURITY CONFERENCE
GROUND ZERO SUMMIT 2013
NOVEMBER 7-10, 2013 | THE ASHOK, NEW DELHI

Security

eScan detects and sinkholes malware domains belonging to Styx EK and SweetOrange EK

InformationWeek, October 25, 2013

From the research done by eScan, it is learnt that the malware attacks are done through drive-by-download method and primarily uses Java / Java applets to initiate the infection

Recommend 0 Tweet

eScan has recently reported that it has detected and sinkholed malware domains belonging to Styx EK and SweetOrange EK that delivered ZBOT, Zero access type of malwares. The main objective of these malwares is to gain foothold into the target systems and deploy other malwares to steal the stored information, insert web-injects, etc.

From the research done by eScan, it is learnt that the malware attacks are done through Drive-By-Download method and primarily uses Java / Java applets to initiate the infection. Domains are specifically registered by the bad actors and servers are hosted to serve the malware. The payloads may vary from Password Stealers to DDOS bots.

For past few months, after actively pursuing Sweet-Orange EK and Styx EK, the research process allowed eScan to discover the domains used by these Exploit Kits (EK) at a consistent rate. Once the malicious domain was identified, eScan initiated a thorough investigation of all the domains associated with this malware campaign.

Apart from this, eScan co-ordinated with the Domain Registrar i.e. PublicDomainRegistry (PDR) and provided them with all the necessary evidences which assisted the compliance team of PDR to suspend these malicious domains. This resulted in take-down of more than 1600 domains. The time dedicated by the research team at eScan to complete this operation was between 72 hours to 10 days.

On this, Govind Rammurthy, MD and CEO, said, "Exploit kits are one of the major threats faced by IT users across all verticals and segments today. The Exploit Kit packs contain malicious programs that are used to carry out automated Drive-by-Download attacks with an aim to spread malware. Legitimate websites are hacked by cyber criminals and malicious code is injected to detect and exploit vulnerabilities of the applications installed on your computer so as to install malicious software that has the capability to compromise the security of all the data on the affected device."

More Insights

Webcasts

The Need for Endpoint Forensics and incident Response in today's evolving threat landscape

SmartCloud Virtualized Server Recovery

More >>

Downloads

Seven Steps for Effective Leadership Development

Back Office Solutions that keep you in front

Deploying Customer Service in the Cloud

More >>