Global Research and Analysis Team

Kaspersky Lab processes more than 325,000 new malicious files every day. While the majority are detected and analyzed automatically, a few require manual input from a security expert. This tiny fraction of the overall files received includes the most sophisticated samples, belonging to the rarest, most menacing new APTs (advanced persistent threats) out there. At Kaspersky Lab, these samples go to the company's expert Global Research and Analysis Team (GReAT).

GReAT is one of Kaspersky Lab's most important assets, bringing together some of the world's best security researchers. Established in 2008, GReAT provides company-wide leadership in anti-malware research and innovation. The security analysts in the team are based around the world, each contributing a unique set of skills and expertise to the research and development of solutions to combat increasingly complex malicious codes. Today GReAT consists of 42 experts working globally and the team has been led by Costin G. Raiu since 2010.

Functions

GReAT conducts incident response during cyberthreat-related events. Key departmental responsibilities include thought leadership in threat intelligence and driving and executing initiatives to improve malicious code detection accuracy rates and efficiency. In addition, the GReAT team supports key customers with threat intelligence expertise.

Security Intelligence

The rise of advanced persistent threats has transformed the global cyber threat landscape, putting critical industrial infrastructure, finance, telecommunications, transportation, research institutes, military contractors, and government networks worldwide at immense risk. These threats are much more complex and stealthy than the average malware, so a different approach is necessary. This is why Kaspersky Lab has GReAT.

Over the last few years, GReAT's combination of expertise, passion and curiosity has led to the discovery of several infamous cyberespionage and cybersabotage campaigns, including Flame, Gauss, RedOctober, NetTraveler, Icefog, Careto/The Mask, Darkhotel, Regin, Cloud Atlas, Epic Turla, Equation and Duqu 2.0. To document all the ground-breaking malicious cyber campaigns that have been investigated by GReAT, Kaspersky Lab introduced a Targeted Cyberattack Logbook.

Technical Expertise / Assisting in Investigations

For some investigations, GReAT works with international organizations such as INTERPOL and Europol, national and regional law enforcement agencies such as the City of London Police and the National High Tech Crime Unit (NHTCU) of the Netherlands' Police Agency, or with Computer Emergency Response Teams (CERTs) worldwide. GReAT helps by assisting in investigations and in the development of countermeasures that disrupt malware operations or cybercriminal activity.

Kaspersky Lab's security experts provide the technical expertise to analyze infection vectors, malicious programs, the Command & Control infrastructure and the exploitation methods supported. Recent joint investigations include fighting cybercrime (such as in the case of Carbanak), disrupting criminal botnets (for example, Simda) and launching the No Ransom initiative.

Kaspersky Lab also partners with companies and organizations such as AlienVault Labs, Dell Secureworks, Crowdstrike, OpenDNS Security Research Team, GoDaddy Network Abuse Department, Seculert, SurfNET, Kyrus Tech Inc. and Honeynet Project, to carry out joint cyberthreat investigations.

Software Vendor Support

One of GReAT's tasks is to actively collaborate with global IT vendors including Adobe, Google, Microsoft and others, in order to coordinate and report discovered vulnerabilities. These are detected through research or by identifying cases "in the wild." Kaspersky Lab supports the IT vendor in addressing the vulnerability by providing it with relevant information and telemetry. The vulnerabilities are reported confidentially and adhere to coordinated disclosure guidelines so that the vendor has time to create and administer a security update patch for its users. In addition, Kaspersky Lab's advanced threat-prevention technologies and vigilant security updates keep its customers protected from the vulnerability until the vendor issues a security patch.

Knowledge Exchange

Kaspersky Lab regularly works with anti-virus researchers across the industry to exchange knowledge about emerging threats. In addition, the company hosts its annual "Kaspersky Lab Security Analyst Summit," which brings together the world's best IT security experts to meet, collaborate and exchange research with international organizations, law enforcement agencies and technology companies. Previous participants include Adobe, Arbor, Barracuda, BlackBerry, Boeing, Google, HB Gary, Interpol, ISEC Partners, Lockheed Martin, and Microsoft.

Kaspersky Lab openly shares its own knowledge, research and technical findings, including indicators of compromise and remediation techniques, with the world's security community, Its online security intelligence hub, Securelist, reports Kaspersky Lab's analytics and has 70 active expert contributors from Kaspersky Lab, making it the world's largest noncommercial security intelligence library.