Global action targeting Shylock malware

By Europol

Published: 2014-07-10 · Archived: 2026-04-05 12:35:14 UTC

On 8 and 9 July 2014, an alliance of law enforcement and industry undertook measures against the Internet domains and servers that form the core of an advanced cybercriminal infrastructure attacking online banking systems around the globe using the Shylock Trojan.

Law enforcement agencies took action to disrupt the system which Shylock depends on to operate effectively. This comprised the seizure of servers which form the command and control system for the Trojan, as well as taking control of the domains Shylock uses for communication between infected computers.

The operation, coordinated by the UK National Crime Agency (NCA), brought together partners from the law enforcement and private sectors, including Europol, the FBI, BAE Systems Applied Intelligence, Dell SecureWorks, Kaspersky Lab and the UK's GCHQ (Government Communications Headquarters) to jointly combat the threat.

Investigative actions were undertaken from the operational centre at the European Cybercrime Centre (EC3) at Europol in The Hague. Investigators from the NCA, the FBI, Italy, the Netherlands and Turkey gathered to coordinate action in their respective countries, in concert with counterparts in Germany, France and Poland. Coordination through Europol was instrumental to taking down the servers that form the core of the botnets, malware and Shylock infrastructure. The CERT-EU (the CERT for the EU institutions, bodies and agencies) participated in the take down and distributed information on the malicious domains to their peers.

During the action several previously unknown parts of the infrastructure were discovered and follow-up actions could be initiated immediately/be set-up and coordinated from the operational centre in The Hague.

Shylock – so-called because its code contains excerpts from Shakespeare's The Merchant of Venice - has infected at least 30 000 computers running Microsoft Windows worldwide. Intelligence suggests that Shylock targets the UK more than any other country, nevertheless the US, Italy and Turkey are also being targeted hard by the malicious code. It is thought that the suspected developers are based elsewhere.

Victims are typically infected by clicking on malicious links, and then persuaded to download and run the malware. Shylock will then seek to access funds held in business or personal bank accounts, and transfer them to the criminal controllers.

Troels Oerting, head of the European Cybercrime Centre (EC3) at Europol, said: *"The European Cybercrime Centre (EC3) is very happy about this operation against sophisticated malware, playing a crucial role in the work to take down the criminal infrastructure. EC3 has provided a unique platform and operational rooms equipped with state-of-the-art technical infrastructure and secure communication means, as well as cyber analysts and cyber experts".*

"In this way we have been able to support frontline cyber investigators, coordinated by the UK's NCA, and working with the physical presence of the United States' FBI and colleagues from Italy, Turkey and the Netherlands, with virtual links to cyber units in Germany, France and Poland."

"It has been a pleasure for me to see the international cooperation between police officers and prosecutors from many countries, and we have again tested our improved ability to rapidly react to cyber threats in or outside the EU. It's another step in the right direction for law enforcement and prosecutors in the EU and I thank all involved for their huge commitment and dedication. A specific thanks goes to Kaspersky Lab who have contributed significantly to the successful outcome of the operation - and our cooperation continues to grow in this and future cases"

Andy Archibald, Deputy Director of the NCA's National Cyber Crime Unit in the UK, said:"The NCA is coordinating an international response to a cybercrime threat to businesses and individuals around the world. This phase of activity is intended to have a significant effect on the Shylock infrastructure, and demonstrates how we are using partnerships across sectors and across national boundaries to cut cybercrime".

Those opting for automated operating system updates - which can ensure computers infected with malware such as Shylock are cleaned automatically following a system restart - need take no action at this time. Those not opting for automatic updates, or who would like to learn more about how to check their Windows-operated computers and remove infections, can go to can go to Microsoft Virus and Security Centre.

Advice on internet security can be found at Cyber Streetwise and Get Safe Online.

For more information, please contact:

EUROPOL
Ms Lisanne Kosters
Corporate Communications
Tel: +31 70 302 5001
