mission control™
security services

OS-CERT
of Open Systems AG

provides Security Analytics and Incident Handling to detect and resolve security breaches that threaten your organization.

Petya malware variant
Mission Control security briefing

Once again, a malware wave has hit IT systems on a global scale, creating disruptions and outages that adversely impacted business. However, out of the million+ systems protected by Mission Control, not a single one was affected. This security briefing explains what happened and why Mission Control customers were safe.

Situation

In the afternoon of 27 June 2017, first rumors about widespread system outages reached Mission Control staff. Through its international network of partners OS-CERT could quickly establish the most likely cause and background.

Timeline (all timestamps are UTC)

14:10	First rumors appear about widespread outages.
14:37	Evidence that malware is spreading through the NSA exploit EternalBlue.
15:04	A sample for analysis is received, confirming the initial suspicion.
16:11	Initial statement published in Mission Control Portal.
17:26	A complete analysis becomes available through trusted channels.
19:00	Updates for customers published.
21:14	In a confidential video conference, security experts from around the world take stock.

Note: As more information was discovered about the malware, its name kept changing. It became known as New Petya, NotPetya and ExPetr.

Thus, in a little more than seven hours, as part of the global security community, Mission Control staff was able to understand and assess the threat. During the incident, Mission Control took preventive measures, e.g. by blocking access to identified download sites.

The malware

Petya was initially distributed through the Ukrainian M.E.Doc software used by many Ukrainian businesses to submit financial data to the government. The M.E.Doc update service was compromised by attackers for this reason. Once inside a network, Petya used different means for lateral movement, hence also infecting sites outside the Ukraine.

Service coverage

OS-CERT provided timely background information to Mission Control that made it possible for customers to protect themselves. Mission Control Security Services help detect and prevent malicious behavior in the following ways:

- The Email Gateway service protects users with the constantly updated, highly agile malware protection feature.
- On the Mission Control Proxy, URLs known to be associated with the malware are blacklisted globally by Mission Control.
- Mission Control Network Security Monitoring has several indicators set in place to maintain visibility and enable swift reaction upon potential compromise. Both indicators for EternalBlue exploit usage, as well as Petya variant malware delivery have been in place since March and April 2017, respectively, and are continuously being updated with latest developments.
- The Mission Control Network Intrusion Prevention service further helps to safeguard against additional infection by blacklisting the infected hosts due to extensive scanning activity, preventing infection of other devices attached via the Mission Control Service Delivery Platform.

If you have any questions, please contact
sales@open.ch

Open Systems AG
Räffelstrasse 29
8045 Zurich

t +41 58 100 10 10
f +41 58 100 10 11
www.open.ch

© 2017, Open Systems AG. All rights reserved. Mission Control™ is a registered trademark of Open Systems AG. Open Systems AG reserves the right to change, modify, transfer, or otherwise revise this publication without notice.