US-CERT CYBER THREAT INFORMATION SHARING BRANCH

CTIS Botnet Operations

Overall Classification: UNCLASSIFIED//TLP AMBER

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

CTIS Counter-Botnet Operational Umbrella

Botnet CNE Operations targeting

- Federal, State , Local, Tribal and Territories enclaves
- Commercial enclaves
- ISACs

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

CTIS Botnet Operations

CTIS Receives internal request for additional threat information

- Activity Report
- Information Bulletin

Collaboration Botnet Operations

- Law Enforcement
- Commercial organizations

Collaboration Products

- Joint Activity Report
- Joint Information Bulletin

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Botnets of Interest

Brobot

- Brobot conducts Distributed Denial of Service (DDoS) attacks targeting online and mobile banking services.

Dridex

- DRIDEX is an online banking malware that steals credential information through HTML injections. Leverages Microsoft Macros. Can be employed to spend spam or participate in DDoS attacks

Past Botnet Collaboration Activities

Brobot

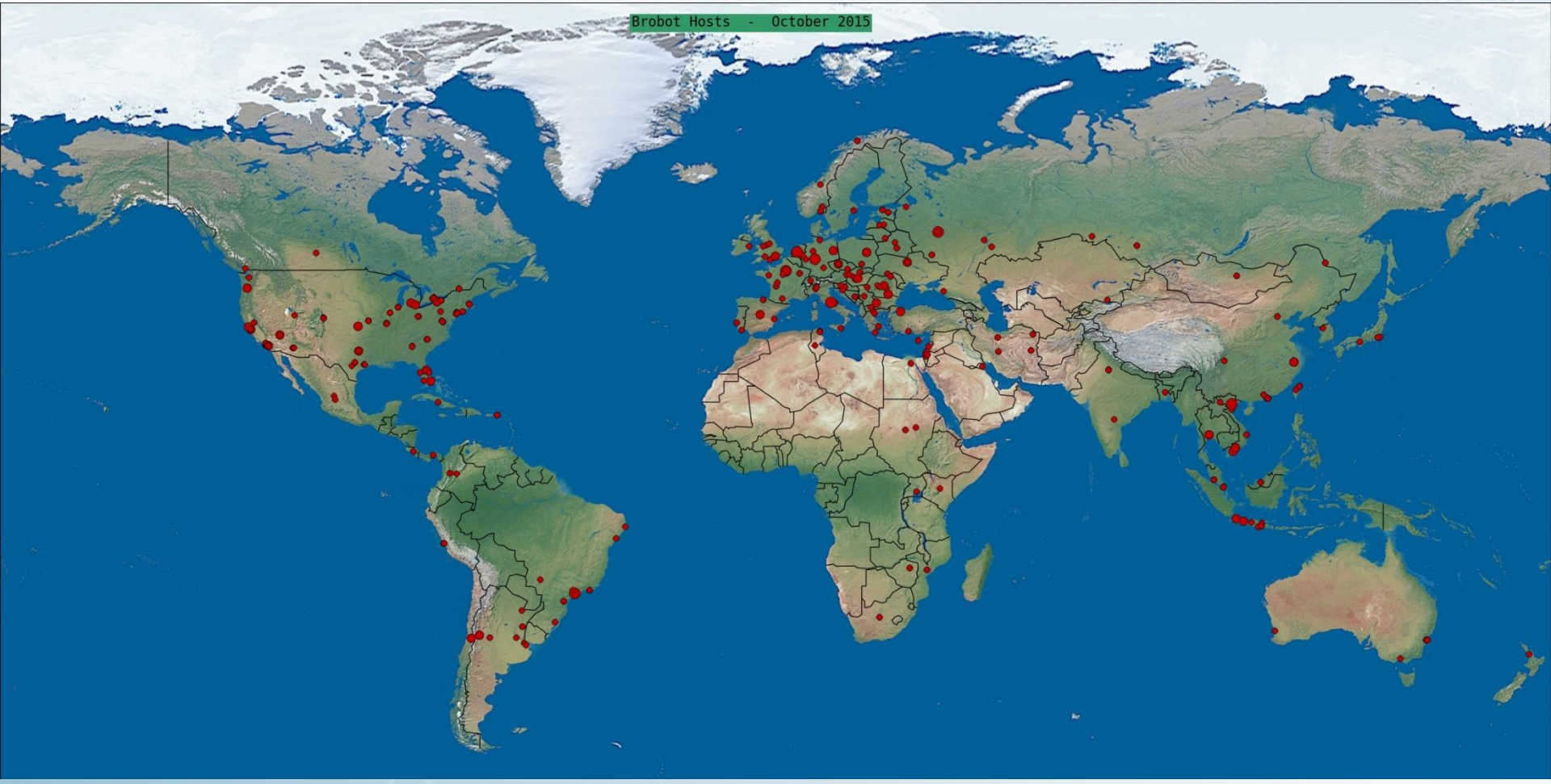
- JAR-15-20151
- 2K+ indicators reported between CTIS US-CERT and Law Enforcement

Dridex

- 1076 victim notification distributed

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

BroBot Hosts Locations



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Top 10 Countries Targeted by Dridex

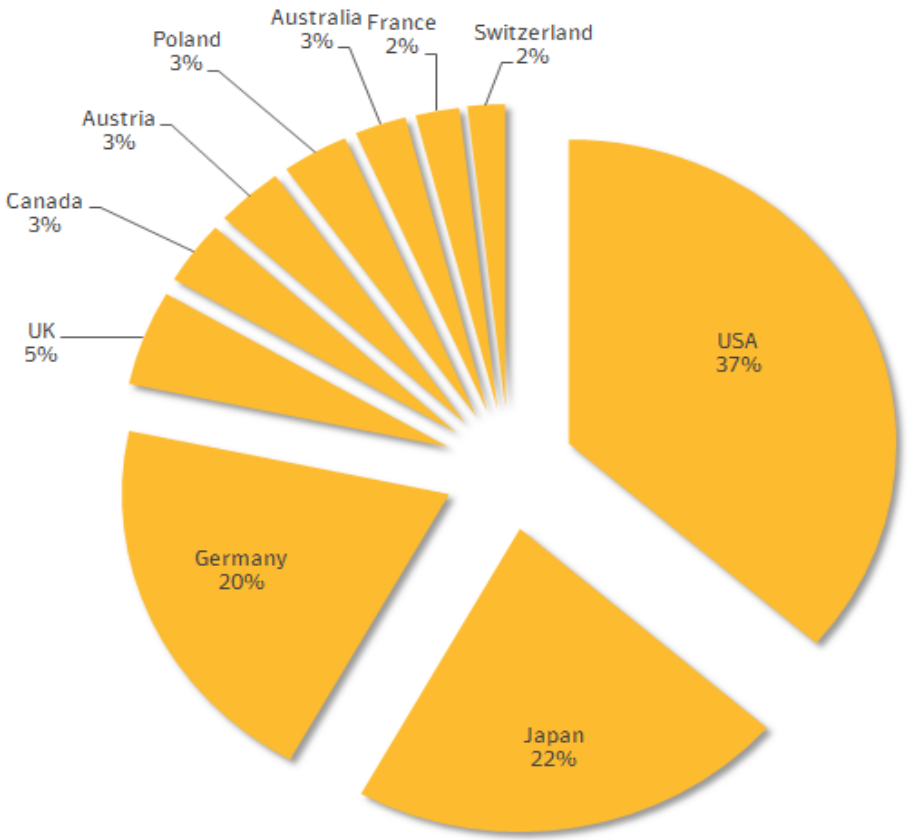


Figure 2. Top ten countries by number of Dridex detections in 2015

CryptoWall v.3 Summary

- First seen in early 2014; infecting machines by January 2015.
- It uses unbreakable AES 256 encryption key.
- Targets 312 file extensions (where previous versions only targeted 146).
- Propagated through phishing campaigns (67.3%) and exploit kits (30.7%); commonly the Angler exploit kit.
- Version 4 now out in the wild.

CryptoWall 3 Snapshot

- 49 unique campaigns in 2015.
- Campaigns “crypt107” and “crypy13” most active.
- 4,546 malware samples discovered.
- 1,213 unique first-tier Command and Control (C2) URLs.
- Five (5) unique second-tier C2 nodes; all located in St. Petersburg, Russia.
- Nearly 406,887 attempted infections observed.
- Accounts for $325 million in damages; victim numbers continue to increase.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT Actions

- NCCIC worked with Law Enforcement on abuse notification list.
- Provided IP addresses to foreign parties.
- Deployed one (1) EINSTEIN 2 (E2) signature.
- All known 1,252 infected victims were notified.

BACKUP

TLP | TRAFFIC LIGHT PROTOCOL

When should it be used?	Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED 	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER 	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN 	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE 	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT Services for Federal Agencies

The United States Computer Emergency Readiness Team strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world. The national CERT offers a variety of services – such as malware analysis, development of machine readable indicators and actionable mitigation approaches, and programs to facilitate information sharing – at no cost to federal agencies.

Analytical Tools & Services

Network & Einstein Analytics: Support the protection of federal civilian agency networks. US-CERT is responsible for monitoring Einstein, a key component of the National Cybersecurity Protection System: an integrated intrusion detection, analysis, information sharing, and intrusion-prevention system. Capabilities will continue to expand at voluntary participating federal agencies. To pursue services, call 888-282-0870 or e-mail the SOC@us-cert.gov.

Incident Reporting Notifications: US-CERT has updated its incident notification guidelines to introduce Threat Vectors and Impact Classifications to replace the old incident categorization taxonomy. These changes align with the release of NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide" and aim to produce higher quality data based on incidents with a confirmed impact. Please report incidents to https://www.us-cert.gov/.

Additional Support Services: US-CERT enables public and private sector partners to identify threats and develop effective security responses.

- *Incident Management:* Within the Federal Government, a cyber incident is defined as a violation of computer security policies, acceptable use policies, or standard computer security practices. To notify US-CERT of an incident, visit: https://www.us-cert.gov/forms/report or e-mail SOC@us-cert.gov.
- *Incident Response:* US-CERT maintains onsite and remote assistance capabilities to provide rapid operational support to respond to and mitigate cyber intrusions and risks.
- *Digital Media and Code Analysis:* The Advanced Malware Analysis Center allows forensic capabilities for US-CERT to exchange and analyze data related to malware threats targeting the U.S. government's network space. To submit malware artifacts for analysis, visit http://malware.us-cert.gov/ or e-mail Virus.Submit@us-cert.gov.

Information Sharing

Interagency Coordination: US-CERT facilitates collaboration for detecting and mitigating threats to the dot-gov domain through several interagency working groups and operational tempo calls.

- *Joint Agency Cyber Knowledge Exchange:* JACKE provides monthly in-person meetings among technical experts from across government security operations centers. The meetings enable detailed discussion of current threats and response strategies.
- *Federal SOC Calls:* US-CERT leads operational coordination calls to discuss trends observed at a tactical level. To participate in the calls, contact notification@us-cert.gov.
- *US-CERT Portal:* US-CERT maintains a secure, web-based collaborative portal to exchange sensitive, cyber-related information and specific technical details regarding incidents on a peer-to-peer level. Membership is open to Federal employees and contractors supporting U.S. government agencies.

US-CERT Publications: Provide subscribers with free, timely information on vulnerabilities, their potential impact, and mitigation to secure computer systems.

- *STIX/TAXII:* International in scope and free for public use, STIX and TAXII are community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time network defense, and sophisticated threat analysis.
- *Indicator Information:* US-CERT creates time-sensitive indicator information about current anomalous and/or malicious cyber activity and disseminates actionable information through Indicator Bulletins and Analysis Reports.
- *Subscriptions:* The National Cyber Awareness System, US-CERT mailing lists, and other feeds offer a variety of information for users.
- *NVD (National Vulnerability Database):* US-CERT manages the U.S. Government's repository of standards-based vulnerability management data.

Cyber Information Sharing and Collaboration Program (CISCP): Provides a systematic approach to cyber information sharing with CI owners and operators. To learn more about the CISCP, contact the US-CERT Operations Center at soc@us-cert.gov.

Information Protection

TLP (Traffic Light Protocol): Provides a set of designations to ensure sensitive information is shared with the correct audience. For full detail on TLP, please visit https://www.us-cert.gov/tlp

Contact US-CERT

US-CERT Security Operations Center
703-235-8856 / 888-282-0870 /SOC@us-cert.gov
Federal Customer Service: federal@us-cert.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM