Mass-malware handling in a National CERT

From information sharing to takedown and interactions with LEA

CIRCL
Computer Incident
Response Center
Luxembourg

Raphaël Vinot - *TLP:WHITE*

CIRCL

September 13, 2016

Who am I

- Raphaël Vinot - @rafi0t
- CERT operator @ Computer Incident Response Center Luxembourg (CIRCL)
- Co-organiser of **hack.lu** - 18th to 20th of October in Luxembourg

CIRCL

- **Government-driven initiative** designed to provide a systematic response facility to computer security threats and incidents.
- CERT for the **private sector**, communes and non-governmental entities in Luxembourg.
- Core team working on **MISP** - http://www.misp-project.org/
- And **MISP ecosystem** - https://github.com/MISP/

Luxembourg, frauds and the financial sector

- Lots of **banks** and financial institutions
- Many intermediaries, managing **big amounts**
- (Broken) English is the default
- Spear phishing
- Fake invoices, or even **fake banks**
- **Banking trojan** such as Dridex

Spear phishing

- **Very targeted** emails or phone calls
- Attacker knows the organisation very well
- **Pressuring** the person responsible to do wire transfers
- Does not work particularly well in small organisations

Banking trojans - Dridex downloaders

- Very **efficient** attackers
  - Sending **massive** amount of **cheap** payloads
  - Use compromised infrastructure
  - **Reused** for different campaigns (Locky and Dridex)
- The vast **majority** of all the dropers come in **emails**
- Active contents: macros, javascript, vba, wsa, ...

Dridex - Downloaders

- New campaigns **every couple weeks** at most in the last 6 months
- Every batch has between 10 and 50 URLs + redirects
- Same compromised website used for Dridex and Locky, serve different binaries
- **Some IPs** are used for over 5 months

Dridex - Downloaders

2016-08-31	Network activity	ip-dst	213.205.40.169	download location	4794 4789 4787 4773 4772 4771 4760 4759 4750 4741 4737 4722 4702 4687 4676 4591 4586 4532 4516 4397 3866	Yes	Inherit
2016-08-31	Network activity	ip-dst	208.71.106.48	download location	4759 4750 4737 4586	Yes	Inherit
2016-08-31	Network activity	ip-dst	212.159.8.91	download location	4794 4586 3183	Yes	Inherit
2016-08-31	Network activity	ip-dst	213.186.33.4	download location	4370 3866 850 845 843	Yes	Inherit
2016-08-31	Network activity	ip-dst	162.210.101.98	download location	4737	Yes	Inherit
2016-08-31	Network activity	ip-dst	81.196.20.133	download location	4759 4516 4404 4397	Yes	Inherit
2016-08-31	Network activity	ip-dst	213.180.150.17	download location	4789 4772 4771 4759 4737 4735 4 4586 4516 4 3331 3026	Yes	Inherit
2016-08-31	Network activity	ip-dst	213.158.72.90	download location	4404 4402		
2016-08-31	Network activity	ip-dst	91.194.151.38	download location			
2016-08-31	Network activity	ip-dst	195.78.215.76	download location	4787 4772 4771 4722	Yes	Inherit
2016-08-31	Network activity	ip-dst	123.242.226.64	download location		Yes	Inherit
2016-08-31	Netw						

Event info: Dridex of the day (2016-02-01) - botnet 223 (incl. private IP addresses)
Correlating Value: 213.180.150.17
date: 2016-02-01

Dridex - TL;DR

- **Over 400 events** related to dridex in our MISP instance
- Few very legitimate looking website with SSL certificates
- Lots of **compromised CMS**
- Nothing fancy, does not make the news, cleaning up is not a priority

Actions on CIRCL's side

- Add all the **indicators into MISP** (once a day)
- **Automatic takedown** requests on the samples (downloaders) we receive
- Follow-up with hosting companies
- Escalate to LEA
- **De-peering** the malicious provider

Hosting companies

- Manual abuse handling is **expensive**, slow down sales and scare customers
- **Inexperienced helpdesk** regarding security incidents
- Very hard to get in touch with the abuse department
  - Protip: Try to talk to the communication department...
- Nobody wants to pay for a cleanup

Law enforcement agencies

- Scaling issues
- Objective: **build a case** against malware authors
- Problems: **flexibility** of the attackers
- Takedown takes a while so potential victims stays at **risk** for a **long time**
- Many different jurisdictions, **hard to build a case**

General technical recommendations

- Use a **dedicated computer** for the wire transfers, with very few applications
- Enforce all network traffic to be directed to and from the banking application
- **Block all active content** from being transferred per **email**
- Always **update** the machine, make sure your provider does the same
- Always **reinstall any compromised device**

Recommendations - Human and organisational

- Have **good communication** within the organisation and take feedback from users
- Build trust relations with your providers so they keep you informed of security issues
- Enforce **dual-signature** for every wire transfer
- Have a policy to ***never* send macros** or any other active attachments
- If you use a smart card: never let it in the reader when not used

Resources

- All the **indicator are available** on CIRCL MISP.
  - https://circl.lu/services/misp-malware-information-sharing-platform/
- Dridex report of CIRCL and other resources:
  - https://www.circl.lu/pub/tr-38/
- **Contact us**: info@circl.lu
  - 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD