

Attackers benefit from sharing information

How can you benefit, too?

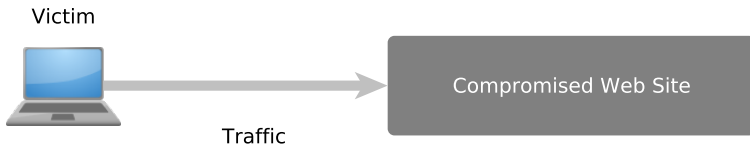


CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy -
TLP:WHITE

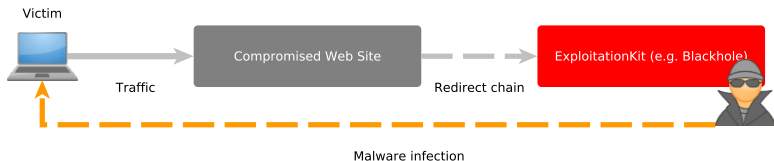
July 4, 2014

How attackers regularly infect Internet users?



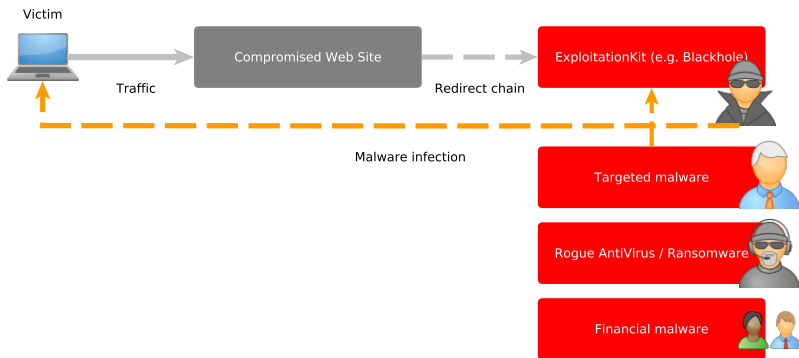
- Abuse vulnerable software (e.g. Web Browsers, plugins, ...)
- Find compromised webservers and install infective payload

What happen behind the scene?



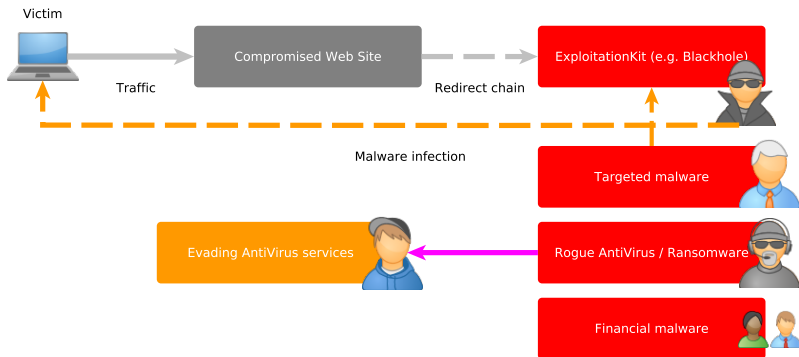
- Attackers industrialize exploitation with exploitation kit (e.g. Blackhole kit)
- Hide their back-office server in a mess of redirect links
- Communicate between the exploitation kit operators and the exploit developers

Targeting users and reselling services



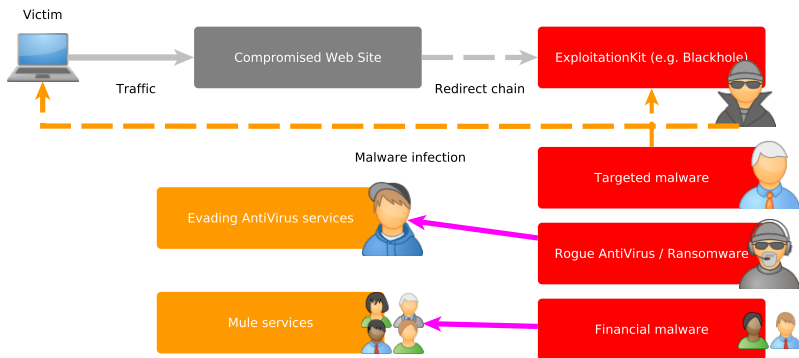
- Attackers get a huge set of (potential) victims classified by country, type, language, operating system...
- They provide services to other customers (e.g. financially attracted attackers, governments, spammers,...)

Is the freshly pushed malware detected?



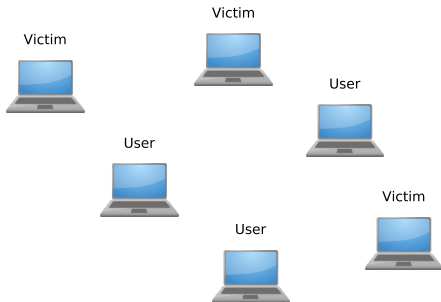
- While new markets emerge, there emerge new services, also for attackers

Getting the money out



- Cash-out is a key element for attackers to get the money out and drop the risks on the mules

Defense and sharing



- Victims or user detecting threats who share can help others to detect/mitigate the threats
- Legal framework, confidentiality can be limiting factors for sharing

Malware Information Sharing Platform (MISP)

- A platform for sharing, storing and correlating Indicators of Compromises (IOCs) of attacks
- Private organizations in Luxembourg or accredited CERTs can request access to their respective MISP platform

The screenshot displays the MISP web interface. At the top, a navigation bar includes links for Home, Core Actions, Feed Filters, Global Actions, Sync Actions, Administration, Audit, Discussions, and Proposals in Overview. The main content area is titled 'Blackshades - bshades RAT'. On the left, a sidebar offers actions like View Event, View Event History, Edit Event, Delete Event, Add Attribute, Add Attachment, Populate from OpenIOC, Populate from ThreatConnect, Contact Reporter, Download as XML, Download as IOC, Download as CSV, and List Events. The event details are as follows:

Event ID	370
Uuid	58776562-260c-4b8b-b117-412591bd210b
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	TLPWHITE
Date	2014-05-15
Threat Level	Low
Analysis	Completed
Distribution	All communities
Description	Blackshades - botnet RAT
Published	Yes

Below the details, there are tabs for 'Fields', 'Attributes', and 'Discussions'. A '370 objects' button is visible. At the bottom, a table lists related events:

Date	Category	Type	Value	Comment	Related Events	ID
2014-05-17	Payload installation	meta	0d1bd381974a4dc0ee668202420a72b		No	

Conclusion

- Attackers are often ahead, sharing and communication plays an important role for their success
- If you share threat intel and indicators, you can:
 - Avoid duplicate analysis work and concentrate on the unknown elements of an attack
 - Automate detection in your infrastructure and reduce the incident response time
- Do you want to share IOCs? Help others and benefit? → info@circl.lu
- PGP Key: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5