Credit-card web-skimming infections can last several months

Threat Memo - Date: 28/02/2020 – Version 1.0

TLP:WHITE

FOR	Category	Type	Domain(s)	Sector(s)	Confidence
INFORMATION	Cybercrime	Web-skimming	World	Digital services, e-Commerce	A1

Key Points

- E-commerce websites infections by credit-card web-skimmers can last several months.
- The lack of security monitoring and reaction to notifications by e-commerce websites' owners constitutes a major risk factor.
- Online shops with large audiences would typically dedicate more resources in patching security flaws and therefore would likely be less risky.

Summary

Since 2015, cyber-criminal groups designated under the umbrella name Magecart have been exploiting vulnerabilities in electronic payment systems, and more specifically the Magento payment software that powers many e-commerce websites, to gain access to customer credit card information in a technique known as card skimming. In December 2013, the Magento payment software was reportedly compromised for the first time. By 2015, the Magecart group began injecting skimmers into vendors' websites and, in 2016 a second group emerged, with a skimmer and infrastructure distinct from the first group.

Several researchers, such as Max Kersten[1], Marco Ramilli[2]and Jacob Pimental[3], are tracking activities of the Magecart groups, especially group 12, which appears to be one of the most active at the moment. They regularly uncover newly infected shopping websites (dozens) and notify owners. However, despite notification, many compromised websites continue running credit card skimming scripts[4], for several weeks or even months. A compilation of known "first infection | last check infection" dates shows, that in some cases, the infection can last up to at least 5 months (see details in Annex). This demonstrates that a major risk factor for the customers is the lack of security monitoring and reactiveness, by the e-commerce website owners.

Some of the high profile websites recently compromised by Magecart group 12 include[5] ticket re-selling websites such as olympictickets2020[.]com and eurotickets2020[.]com. In an effort to avoid detection or make analysis more difficult, the group is frequently changing its techniques or infrastructures when discovered and exposed in researchers' blogposts. This includes:

- Changing domains where skimming code is hosted, typically when the hosting domain is taken down,
- Changing address of the hosting domain,
- Changing skimming code (e.g. in one campaign it changed four times),
- Changing encoding to mask / obfuscate skimming code or URL (e.g. charset differentiation, junk code to spear random comments making quite hard the overall reading)

Comments

MageCart attacks have increased in recent years, affecting hundreds of thousands of websites. Magecart groups usually do not select their targets, they mostly attempt to compromise any e-commerce websites they encounter.

Online shops with large audience will typically dedicate more resources in patching security flaws, running periodic audits, and react faster when notified by researchers. Therefore, while visiting e-commerce websites of smaller shops, users should be careful when providing card details and sensitive data, which are more likely to fall prey to web skimmers.

IT administrators running e-commerce websites can avoid the threat or at least minimize the risk if they update the software when a new release becomes available. Furthermore, providing a communication line to be notified by security researchers could not only avoid customers from becoming victims but could also improve maintaining a more secure website.

[1] https://maxkersten.nl/2020/02/24/closing-in-on-magecart-12/
[2] https://marcoramilli.com/2020/02/19/uncovering-new-magecart-implant-attacking-ecommerce/
[3] https://www.goggleheadedhacker.com/blog/post/16
[4] https://www.bleepingcomputer.com/news/security/credit-card-skimmer-running-on-13-sites-despite-notification/
[5] https://www.riskiq.com/blog/labs/magecart-group-12-olympics/

Compromised Website	First infection detected	Still infected until at least	Minimum compromised days
Suplementos Gym	Jan 31, 2020	Feb 20, 2020	20
Bahimi swimwear shop	Nov 2019	Feb 20, 2020	111
TitansSports (sports glasses)	Early Jan 2020	Feb 20, 2020	50
BVC	Feb 3, 2020	Feb 20, 2020	17
MyMetroGear	Feb 4, 2020	Feb 20, 2020	16
Fashion Window Treatments	Feb 6, 2020	Feb 20, 2020	14
Skin Trends	Feb 6, 2020	Feb 20, 2020	14
BioPets	Sept 30, 2019	Feb 25, 2020	148
Wellspring Wholesale	Sept 30, 2019	Feb 9, 2020	132
Wellspring Customer	Sept 30, 2019	Feb 9, 2020	132
D2D Organics	Sept 30, 2019	Nov 1, 2019	32
Loud Shirts USA	Oct 1, 2019	Feb 9, 2020	131
Nilima Home	Oct 1, 2019	Feb 9, 2020	131
Silk Naturals	Oct 1, 2019	Feb 16, 2020	138
JD's Sound & Lighting	Oct 2, 2019	Feb 9, 2020	130
Nilima Rugs	Oct 2, 2019	Feb 10, 2020	131
The Cheshire Horse	Oct 6, 2019	Dec 11, 2019	66
The Top Collection	Oct 19, 2019	Feb 25, 2020	129
Selaria Dias	Nov 5, 2019	Feb 21, 2020	108
Tile	Nov 13, 2019	Feb 25, 2020	104
Liquorish Online	Nov 13, 2019	Nov 24, 2019	11
Sport Everest	Nov 20, 2019	Feb 25, 2020	97
ABC School Supplies	Nov 26, 2019	Feb 10, 2020	76
Motor Book World	Nov 26, 2019	Feb 22, 2020	88
Giocattoli Negozio	Dec 12, 2019	Feb 25, 2020	75
SoleStar	Jan 11, 2020	Feb 25, 2020	45
Surf Bussen Travel	Jan 17, 2020	Feb 10, 2020	24
Haight Ashbury Music Center	Jan 24, 2020	Feb 18, 2020	25
MyCluboots	Jan 25, 2020	Feb 25, 2020	31
Parkwood Middle School Bears	Jan 31, 2020	Feb 25, 2020	25
Voltacon	Feb 12, 2020	Feb 25, 2020	13
Pitcher's Sports	Feb 13, 2020	Feb 25, 2020	12
Powerhouse Marina	Feb 13, 2020	Feb 25, 2020	12
ZooRoot	Feb 14, 2020	Feb 25, 2020	11
Integral Yoga Distribution	Feb 18, 2020	Feb 25, 2020	7
Kitchen And Couch	Feb 19, 2020	Feb 25, 2020	6