GRAPHUS OUTPERFORMS MICROSOFT ATP FOR A LARGE, GLOBAL ENTERPRISE

Automated Phishing Defense powered by the TrustGraph®

GRAPHUS OUTPERFORMS MICROSOFT ATP FOR A LARGE, GLOBAL ENTERPRISE

GLOBAL ORGANIZATION WAS GETTING TARGETED WITH HIGHLY SOPHISTICATED PHISHING ATTACKS

Graphus was asked to support a global organization with over 3,000 employees and over $2 billion in annual revenue. This organization was using Microsoft's Office 365 cloud email platform and also had Advanced Threat Protection (ATP) implemented and they were seeing nearly 1,500 spoofing, phishing, scam, and even malicious attacks every year. These attacks were highly sophisticated, zero-day attacks getting past ATP and making it to their employees. Moreover, the attacks took hours, sometimes days, for browsers and ATP to detect and block. Allowing these attacks to be active for hours or days is a massive risk to any organization, especially when the average time it takes someone to click on a phishing link is 16 minutes! They knew something had to change. They decided to activate Graphus® for an added layer of protection and immediately saw the value.

3,000+
EMPLOYEES

$2B+
REVENUE

USING
OFFICE 365
& ATP

MANY ORGANIZATIONS ARE FACING SIMILAR PROBLEMS

The problem this organization was facing, like many organizations we work with today, was no matter how they had ATP configured and the various rules they had in place, attacks were still slipping by and reaching their employees. This comes down to the fundamental approach to this massive problem. But why are these attacks able to make it past ATP and other technologies? Because, ATP, like many tools available today, rely on insufficient traditional detection mechanisms such as threat intelligence, sender reputation, DMARC, and heuristics. Threat intelligence is cybersecurity threat information that is already known. It may come from open source intelligence, social media intelligence, the dark web, or elsewhere, but the key fact is, it has already been identified as a threat or an attack. This can be valuable information, which is why so many solutions rely on this data for their detection capabilities, however there are two critical problems with using tools that rely on traditional detection mechanisms.

First, the bad guys know these detection mechanisms. They have access to the same intelligence and tools. They are extremely skilled and know how to navigate these technologies and reach your employees - which is why this is a multi-billion dollar business for them.

Second, technologies that detect KNOWN threats only solves half the problem. What about the UNKNOWN threats? The highly sophisticated, zero-day attacks? With nearly 46,000 new phishing sites created every day and the ever-changing attack strategies developed by these skilled attackers, it's impossible for traditional solutions to keep up. This is where Graphus® differs. It doesn't rely on traditional detection mechanisms. It leverages proprietary and patented AI technology, the TrustGraph®, to detect both known AND unknown attacks.

GRAPHUS OUTPERFORMS MICROSOFT ATP FOR A LARGE, GLOBAL ENTERPRISE

GRAPHUS ACTIVATED IN MINUTES AND DEVELOPED A TRUSTGRAPH UNIQUE TO THEIR ORGANIZATION

This global organization was able to get Graphus® activated on Office 365 in a matter of minutes. Their TrustGraph® instantly began to analyze historical interactions and assign trust-ratings and unique fingerprint to senders. Once their TrustGraph® initialized, Graphus® began analyzing incoming messages in real-time. Within a matter of minutes, Graphus® was able to detect the first, of many, confirmed attacks which was missed by Microsoft ATP and delivered straight to the inbox of one of their employees.

ACTIVATED IN MINUTES

UNIQUE TRUSTGRAPH

GRAPHUS OUTPERFORMS MICROSOFT ATP FOR A LARGE, GLOBAL ENTERPRISE

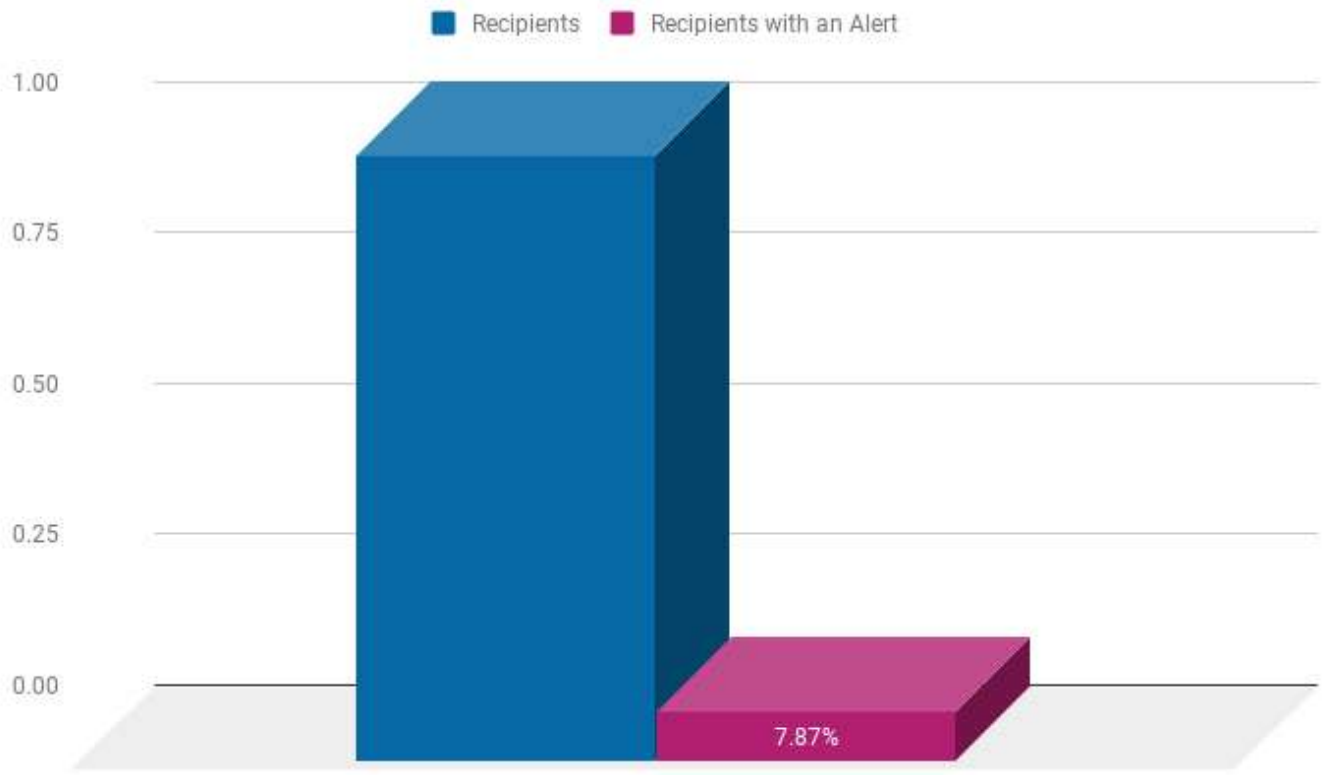
GRAPHUS BY THE NUMBERS

Once Graphus® was activated, they immediately saw the value. During the first two weeks Graphus® generated the following metrics:

An average of 22,000 emails processed each day with less than 10 alerts generated each day.

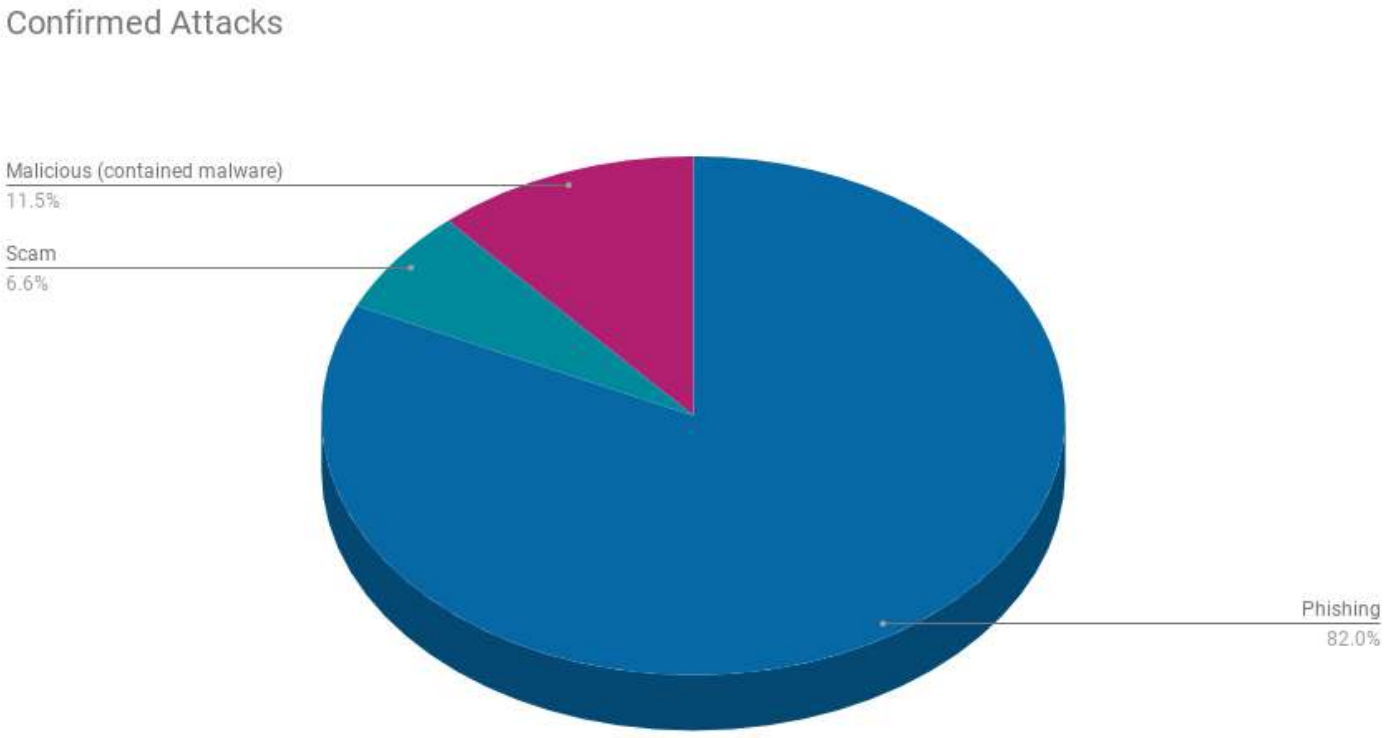
ALERTS GENERATED

Less than 8% of the employees saw an alert during this two week period. Graphus® is well below the industry average when it comes to number of false positives.



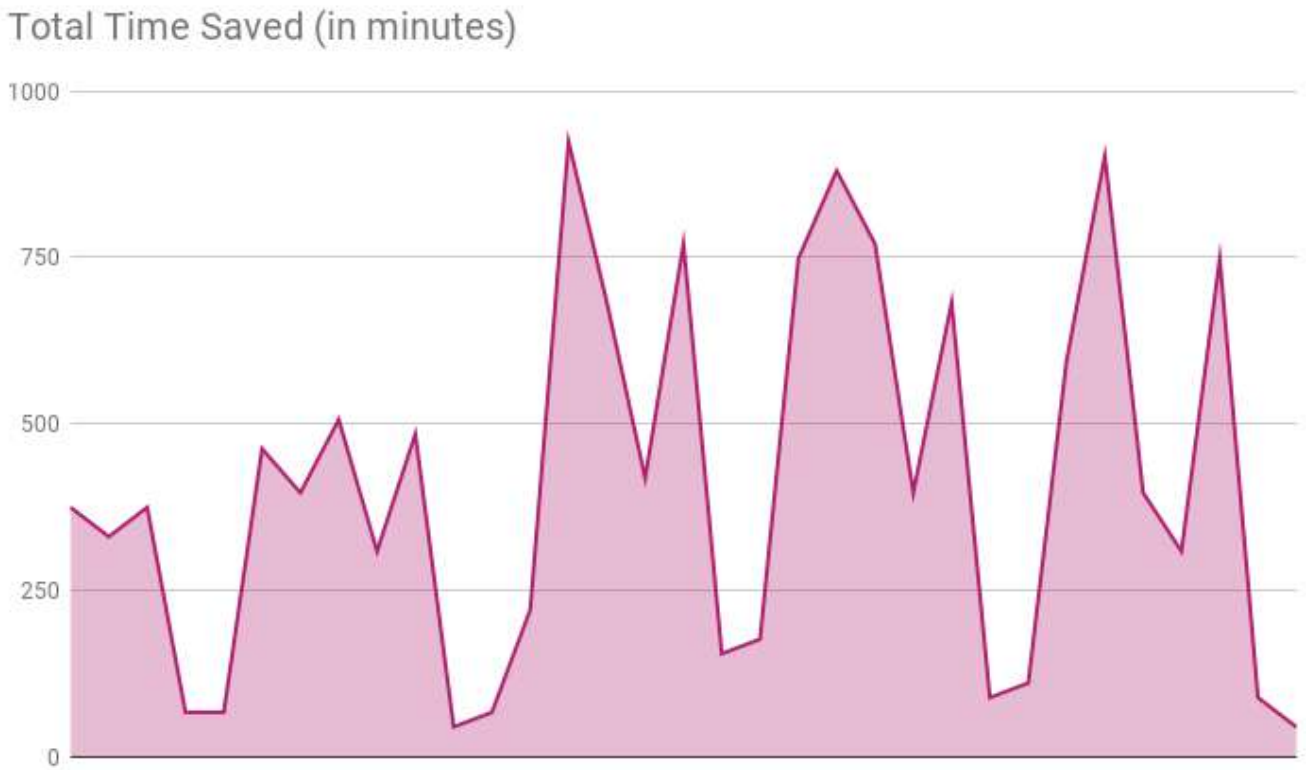
CONFIRMED ATTACKS

Graphus® detected 61 confirmed attacks. These were highly targeted phishing, scam, and malicious attacks that slipped past ATP.



EMPLOYEESHIELD™ VALUE ADD

EmployeeShield™ helped reduce the information security teams workload by 84%. Graphus® saved this organization nearly 13,000 minutes during this two week period.



GRAPHUS OUTPERFORMS MICROSOFT ATP FOR A LARGE, GLOBAL ENTERPRISE

THE ROI OF GRAPHUS

These insights reveal that within a short period of time, Graphus® was able to detect 61 attacks that slipped past ATP and the Microsoft Office 365 rules this organization has in place. It also reveals that their employees are taking action through EmployeeShield™, our interactive warning banners, which has reduced the information security teams workload by 84%!

61 TARGETED ATTACKS DETECTED WITHIN THE FIRST 2 WEEKS

84%

REDUCTION IN IT/SECURITY WORKLOAD

ABOUT GRAPHUS

Graphus® is the industry's first automated phishing defense platform that provides immediate protection against spear phishing, phishing, business email compromise, and malware attacks. It is powered by TrustGraph® – a unique, powerful, and patented AI technology. Companies can activate Graphus® in minutes. For more information, please visit www.graphus.ai.

REFERENCES:
https://www.graphus.ai/where-secure-email-gateways-fail-graphus-excels/
https://www.graphus.ai/securing-last-line-defense-graphus-phishing-awareness-training-solutions/