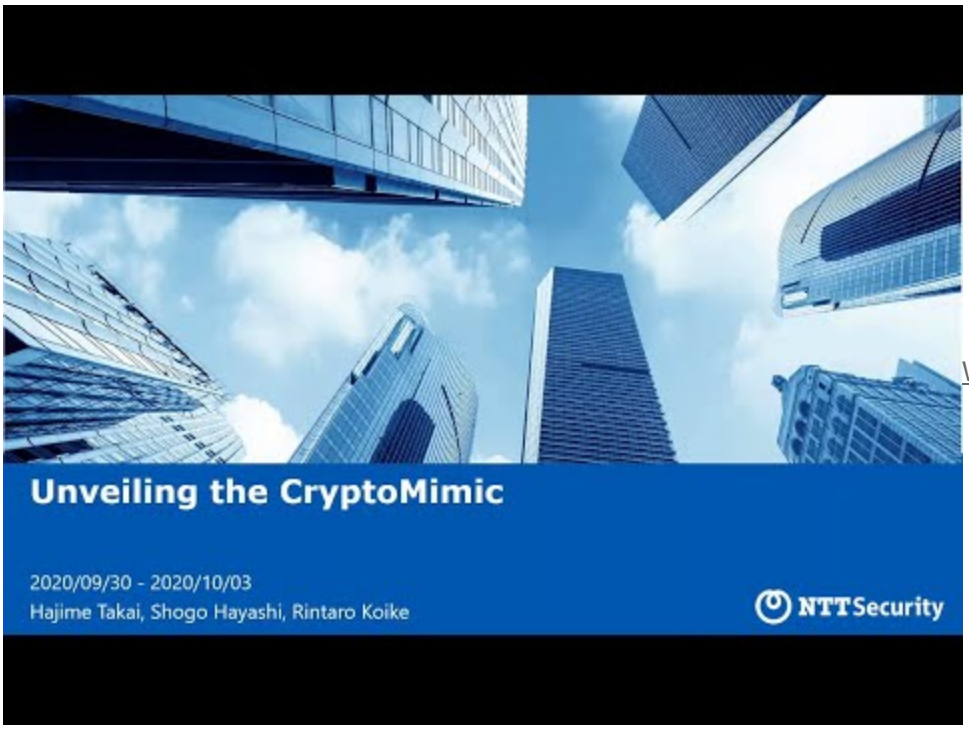
Unveiling the CryptoMimic

vb2020.vblocalhost.com/conference/presentations/unveiling-the-cryptomimic/

Hajime Takai (NTT Security), Shogo Hayashi (NTT Security) & Rintaro Koike (NTT Security)



Watch Video At:

https://youtu.be/8K_aG1d6dzo

ANY.RUN - Interactive malware analysis sandbox

Avira Cloud Sandbox API. Completely private, unlimited-scale, automated malware analysis service

Supports MITRE ATT&CK™ framework.

partner message

Do APT Mercenary Groups Pose Real Threat to Companies?

https://businessresources.bitdefender.com/apt-as-a-service-webinar
Learn about the recent Bitdefender investigation of a new attack attributed to a sophisticated actor offering advanced-persistent-threats-as-a-service.

Access the investigation

partner message

Be a part of the cyber resilience story - explore careers at

https://careers.opentext.com/
Join the cybersecurity and data protection team at Carbonite + Webroot, OpenText companies.

partner message

We don’t just talk about sharing. We do it every day

https://www.cyberthreatalliance.org/our-sharing-model/
Find out more about how threat intelligence sharing and collaboration through the Cyber Threat Alliance can function as a force multiplier to improve defenses across the ecosystem.

partner message

Map Malicious Infrastructures with Pure Signal™ Intelligence

https://partners.team-cymru.com/pure-signal-trial
Elite analyst teams use Team Cymru’s Pure Signal platform to access 50+ data types, including global network flow, PDNS, malware and more.

Start your 2-week trial now!

partner message

What is cyber threat intelligence (CTI) and how is it used?

Join the VB2020 Threat Intelligence Practitioners’ Summit (TIPS)
Join the VB2020 Threat Intelligence Practitioners’ Summit, sponsored by the Cyber Threat Alliance,

to hear from leading industry voices on how CTI sharing can function as a force multiplier to strengthen defenses across the ecosystem.

partner message

Kaspersky Threat Intelligence Portal - find cyberthreats in files, URLs, IPs and domains

https://opentip.kaspersky.com/
Know which alerts or incidents pose real threats, and prioritize them fast and effectively based on impact and risk levels.

partner message

No-Cost Threat Detection for ISPs and Hosting Providers

https://partners.team-cymru.com/nimbus-threat-monitor
Partner with Team Cymru and get near-real-time threat detection, powered by our world-class IP Reputation data.

Join us now!

partner message

Outsource your Unwanted Software/PUA Work for Free

https://appesteem.com/avs
AppEsteem's feeds sort out the good apps from the Deceptors.

Our criteria are widely accepted. We'll help with your disputes.

All for Free. Giving you more time to fight real malware.

partner message

Do you want to know how IT security products score in independent tests?

https://www.av-comparatives.org/enterprise/latest-tests/
AV-Comparatives is an ISO certified independent organization offering systematic testing that checks whether security software lives up to its promises.

Results are available for free!

partner message

Downloads

- Download paper (PDF)
- Download slides (PDF)

CryptoMimic (also called Dangerous Password） is an APT actor observed since around March 2018. It is reported that CryptoMimic attacks worldwide companies and organizations, especially targeting crypto currency companies. Several security researchers all over the

world had already published reports on this attack, but they only dealt with the initial part of the attack. CryptoMimic is very careful and it is extreamely difficult to observe the attack under virtual environments including sandbox. As a result, there has been no detailed report that deals with the malware that the attacker finally executes or how it behaves during the attack.

In this presentation, we will reveal the analysis result of unknown malware never reported before and the picture of the whole attack. In this presentation, we first introduce two initial samples (LNK file and macro-embedded *MS Office* file) used by CryptoMimic. Then, focusing on the attack using LNK file, we disclose the whole picture of CryptoMimic that we observed in February 2020.

We detail how the attack proceeds from initial sample to final malware execution along with the results of analysis of the attacker's behaviours and executed malware. We also found various metadata that the attacker left on the victim. By leveraging the metadata, we also try to unveil the attacker's profile or attribution.

Finally, we share Yara rules and characteristics of the attack for defending or threat hunting. Through this presentation, SOC, CSIRT and security researcher will be able to have deeper understanding on the attack by CryptoMimic and gain knowledge on how to detect or defend against the attack.

Hajime Takai

NTT Security

Hajime Takai currently works as a SOC analyst and a malware researcher at *NTT Security (Japan) KK*. He joined *NTT Security* in 2016, before which he worked for five years as a software engineer. He contributes to the *NTT Security* blog about malware research. He has written a white paper about Taidoor in Japanese. He has presented at Japan Security Analyst Conference 2020. He loves mahjong.

Shogo Hayashi

NTT Security

Shogo Hayashi has worked as a SOC analyst for more than 10 years at *NTT Security (Japan) KK*. His main specialization is responding to EDR detections, creating IoCs, malware analysis and researching endpoint behaviour of threat actors. In addition, he posts articles and whitepapers in NTT Security. He is a cofounder of SOCYETI, an organization for sharing threat information and analysis technique to SOC analysts in Japan.

Rintaro Koike

NTT Security

Rintaro Koike is a security analyst at *NTT Security (Japan) KK*. He has been engaged in SOC and malware analysis. In addition, he is the founder of 'nao_sec'. He always collects and analyses threat information. He has been a speaker at Japan Security Analyst Conference 2018/19/20, HITCON Community 2019, VB 2019, AVAR 2019, CPRCon 2020 and Black Hat USA 2018 Arsenal.

← Back

Hajime Takai (NTT Security), Shogo Hayashi (NTT Security) & Rintaro Koike (NTT Security)

CryptoMimic (also called Dangerous Password） is an APT actor observed since around March 2018. It is reported that CryptoMimic attacks worldwide companies and organizations, especially targeting crypto currency companies. Several security researchers all over the world had already published reports on this attack, but they only dealt with the initial part of the attack. CryptoMimic is very careful and it is extreamely difficult to observe the attack under virtual environments including sandbox. As a result, there has been no detailed report that deals with the malware that the attacker finally executes or how it behaves during the attack.

In this presentation, we will reveal the analysis result of unknown malware never reported before and the picture of the whole attack. In this presentation, we first introduce two initial samples (LNK file and macro-embedded *MS Office* file) used by CryptoMimic. Then, focusing on the attack using LNK file, we disclose the whole picture of CryptoMimic that we observed in February 2020.

We detail how the attack proceeds from initial sample to final malware execution along with the results of analysis of the attacker's behaviours and executed malware. We also found various metadata that the attacker left on the victim. By leveraging the metadata, we also try to unveil the attacker's profile or attribution.

Finally, we share Yara rules and characteristics of the attack for defending or threat hunting. Through this presentation, SOC, CSIRT and security researcher will be able to have deeper understanding on the attack by CryptoMimic and gain knowledge on how to detect or defend against the attack.

Hajime Takai

NTT Security

Hajime Takai currently works as a SOC analyst and a malware researcher at *NTT Security (Japan) KK*. He joined *NTT Security* in 2016, before which he worked for five years as a software engineer. He contributes to the *NTT Security* blog about malware research. He has written a white paper about Taidoor in Japanese. He has presented at Japan Security Analyst Conference 2020. He loves mahjong.

Shogo Hayashi

NTT Security

Shogo Hayashi has worked as a SOC analyst for more than 10 years at *NTT Security (Japan) KK*. His main specialization is responding to EDR detections, creating IoCs, malware analysis and researching endpoint behaviour of threat actors. In addition, he posts articles and whitepapers in NTT Security. He is a cofounder of SOCYETI, an organization for sharing threat information and analysis technique to SOC analysts in Japan.

Rintaro Koike

NTT Security

Rintaro Koike is a security analyst at *NTT Security (Japan) KK*. He has been engaged in SOC and malware analysis. In addition, he is the founder of 'nao_sec'. He always collects and analyses threat information. He has been a speaker at Japan Security Analyst Conference 2018/19/20, HITCON Community 2019, VB 2019, AVAR 2019, CPRCon 2020 and Black Hat USA 2018 Arsenal.